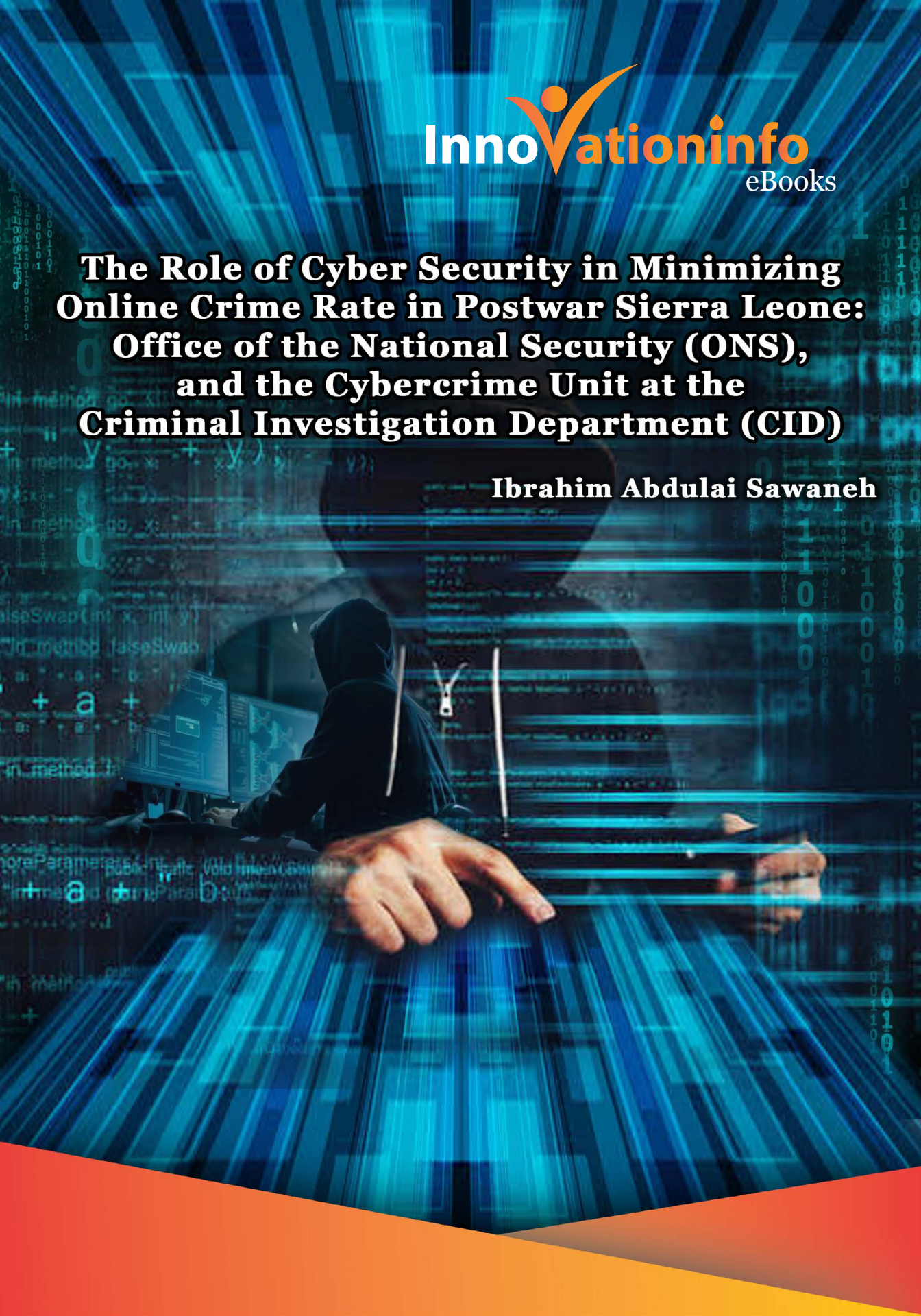
InnoVationinfo
eBooks

The Role of Cyber Security in Minimizing Online Crime Rate in Postwar Sierra Leone: Office of the National Security (ONS), and the Cybercrime Unit at the Criminal Investigation Department (CID)

Ibrahim Abdulai Sawaneh



The Role of Cyber Security in Minimizing Online Crime Rate in Postwar Sierra Leone: Office of the National Security (ONS), and the Cybercrime Unit at the Criminal Investigation Department (CID)

Author

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone.

ISBN: 978-1-63278-972-3

DOI: 10.4172/978-1-63278-972-3

Published: December 2019

Printed: December 2019

Published by Innovationinfoebooks

Heathrow Stockley Park,

Heathrow UB11 1BD, UK

CONETENTS

PREFACE

The main reason for carrying out this piece of work was stemmed out of the passion gained during my postgraduate studies, and to help the government and its agencies/departments to legislate strong cyber policies that would safeguard the nation from imminent cyber-attacks and information security breaches. As globalization engulfed planet earth with more new technological terminologies such as digitalization, block-chain technology, information age, Internet of Things (IoT), big data technology, Bitcoin technology, all generating massive data sets that are transmitted over the Internet. Security issues to mind, especially for countries with weak IT infrastructures to mechanize proactive steps that would withstand cybercrime and its related online frauds. The government should enact laws that will prescribe punishment for perpetrators of online crimes and also introduces cyber studies in schools to create awareness among the country's population. Therefore, the research will focus on the various preventive methods that would deter or mitigate the cybercriminals from actively committing such crimes within the Sierra Leone cyberspace. The author would, therefore, like to acknowledge those who contributed to the success of this work especially the two research institutions. A special thanks go to the academic staff of the Atlantic International University, USA. Furthermore, much appreciation is due to Mrs. Elizabeth Guma-Sawaneh for her financial and moral support during these turbulent times. Profound appreciation is also accorded to Prof. Paul Kamara (dad) and Professor Roseline Emeh Uyanga of the Institute of Advanced Management and Technology (IAMTECH) Sierra Leone, Professor Edwin J.J Momoh, Vice-Chancellor at the Ernest Bai Koroma University of Science and Technology (EBKUST) Sierra Leone, and finally to my supervisor Professor Prince Sorie Conteh, Director of Research at the University of Sierra Leone. Ibrahim Abdulai Sawaneh.

Ibrahim Abdulai Sawaneh

ACKNOWLEDGMENT

It was not an easy task in writing this thesis, because of limited resources internally. The researcher, therefore, conducted an extensive interview and distributed questionnaires to the Cybercrime Unit at the Criminal Investigation Department of the Sierra Leone Police Force and ONS. The author, therefore, would like to acknowledge these institutions for providing relevant information that was used to complete this piece of research, especially Tity Kamara and Lansana M. Marah respectively. I would also like to thank my coordinator Dr. Nick Karimi, tutor Dr. Deborah Rodriguez, and admission officer Keren Feliciano from the Atlantic International University, USA. Furthermore, much appreciation is due the Mrs. Elizabeth Guma-Sawaneh for her financial and moral support. Profound appreciation is also accorded to Prof. Paul Kamara and Professor Roseline Emeh Uyanga of the Institute of Advanced Management and Technology (IAMTECH), Professor Edwin J.J Momoh, Vice-Chancellor and Principal of the Ernest Bai Koroma University of Science and Technology, my supervisor, Professor Prince Sorie Conteh, Director of Research at the University of Sierra Leone, Dr. Musa Tarawally, a lecturer at the Ernest Bai Koroma University of Science and Technology, and Assistant Professor Nadir Mustapha Usman from the University of Blue Nile in Sudan.

Notice

Statements and opinions expressed in the book are these of the individual contributors and not necessarily those of the editors or publisher. No responsibility is accepted for the accuracy of information contained in the published chapters. The publisher assumes no responsibility for any damage or injury to persons or property arising out of the use of any materials, instructions, methods or ideas contained in the book.

Additional hard copies can be obtained from orders

@https://www.innovationinfobooks.com/

ABOUT THE BOOK

This thesis investigates the role of cybersecurity in postwar Sierra Leone and assesses its impacts on the economic development and improvement of the security challenges related to cybersecurity in the country. Modern technology has made humankind lazy and one cannot go without it. Most nations rely heavily on the internet to perform their day-to-day operations, and this has made operations easier for them. Unfortunately, this same technology harms societies depending on the intention of the users. As we are living in a global digital age, with everything interconnected to the network of networks, raises urgent concern. We have seen numerous global cyber-attacks that have resulted in huge financial loss and cyber defense. These attacks and threats continue to increase because most nations, organizations, and individuals depend on these digital systems for their day-to-day activities. An organized Internet crime with more sophisticated cyber hacking techniques poses greater threats to societies and nations. Individual nations and organizations are faced with critical issues on how to defend their cyberspace. Cybercrime as a digitized stage for performing political espionage and cyber warfare is the new global order. A qualitative data analysis method was applied. Interview and questionnaire schemes were adopted in collecting the required data for the research. The Office of the National Security (ONS) and the Cybercrime Unit at the Criminal Investigation Department were the two (2) targeted institutions for this research. The investigation of the thesis concludes that there is no legislation or laws relating to cybersecurity and cybercrime in the country. Though there have been draft legislation conducted in 2016, it is yet to be enacted into law. Therefore, the researcher provides solutions to tackle the challenges and threats faced by utilizing cyberspace. Fortunately, the awareness of information and communications technology (ICT) uses in higher educational institutions and key government departments have raised more consciousness on how state and individual data should be protected. This is essential as internet criminals are well trained and equipped with modern technologies to access peoples' personal information, and use it illegally. Understanding cyber risks are essential for minimizing the cybercrime rate in postwar Sierra Leone. Cyber-attacks are gradually on the rise and it is regarded as a national security matter. Though it seems too complex to design an effective measure to protect and secure the cyberspace, this thesis exhibits several security options that can withstand the numerous cybersecurity threats and challenges nationwide.

Keywords: Scientific Support Department (SSD), Office of the National Security (ONS), Cybercrime, Cyber Security, Cyberspace.

Chapter 1
General Background to the Research

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

[*]**Corresponding author:** Ibrahim Abdulai Sawaneh, Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

Introduction

Cybercrime is a terminology that describes the act of using cyberspace to steal or cause mayhem to people, organizations and/or governments via computer technology. It is mostly done via the internet where attackers invade a computing system to steal sensitive data, corrupt systems by viruses' infections, botnets, and various email scams [1].

The advancement in ICT is alarmingly growing concerning how it is managed, especially in developing countries such as Sierra Leone. This as a result of the internet and the World Wide Web (WWW) with everything interconnected in the cyberspace. Cyberspace is the new trend in the global village having both negative and positive impacts. Until now, there is no globally accepted definition for cyberspace that involves software domain, hardware platform, the network of networks (Internet), servers, Internet of Things (IoT), computing systems, cloud computing, informatization, big data technology, telecommunications, mobile computing, nations, corporations, and people. It involves all the activities carried out in the cloud. This process has engulfed virtually every aspect of human interactions or activities ranging from e-health, teleconferencing, e-commerce, e-learning, e-transportation, smart homes, smart cities, education, governance, administration, management, agriculture, and e-banking.

The continuous technological innovations in all facets of life bringing people connected through the Internet, thereby interconnecting different regions to the other, as well as, industries and state actors globally [1]. Importantly, cheaper electronic devices such as mobile phones, other electronics, and electrical gadgets are making a huge impact on how people see and appreciate them. Based on the numerous cyber-attacks [2, 3] faced by several governments and entities around the world prompted the Government of the Republic of Sierra Leone to enact several cybersecurity departments to deal with Internet security issues.

The Ons

The ONS was established by the government of Sierra Leone to fight cybercrimes in 2002 and has since managed to minimize cybercrime within the cyberspace of Sierra Leone. Before the establishment of ONS, there was a special branch within the Sierra Leone Force responsible for security matters (Counter-Espionage, Counter-Terrorism, and Counter-Subversion)[1].

Unfortunately, they were only concerned with monitoring political party activities, student unionism, and trade unionism, forgetting about the effects of online criminals. As a result, the government of Sierra Leone enacted a national policy to guide and protect the nations' from imminent cyber-attacks.

The cybercrime unit

The cybercrime unit was established in the 2000s and mandated for tracking online criminals who hacked into people's mobile phones, either to steal sensitive data that may have devastating effects on individuals or organizations and /or just to incapacitate the operations of people's comfort. This is the most common online crime in Sierra Leone, as majorities do not have adequate knowledge of cyberspace and cybercrime-related issues. People normally blackmail politicians especially during national elections, as seen in the 2018 Presidential and Parliamentary elections in Sierra Leone.

The Sierra Leone National Telecommunications Commission (NATCOM), and the Ministry of Information and Telecommunications worked together to tackle online crime in Sierra Leone. With the end of the civil war that ravaged Sierra Leone between 1991 and 21001, Sierra Leone has gradually experienced security threats and challenges, especially the internet and its related domains [4].

The goal of the study is to help minimize the cybercrime rate in Postwar Sierra Leone. The Cyberspace defense scheme is geared towards a single model for nations with formidable and organized structures. With weak IT infrastructures, the country faces several security risks and challenges within cyberspace. ICT Policymakers in the country referred to the existing regulations as ineffective and not viable, because the existing schemes are outdated. The research geared towards providing best practice that detects and tackles key challenges faced by existing structures, including affordability of devices, and availability of experienced cybersecurity staff. Moreover, the challenges encountered in the area of internet security are imminently different from those faced by other nations.

The Internet greatly transformed people's lives thereby improving the development and sustenance of a nation. These improvements are attributed to new technological innovations with numerous benefits. Notwithstanding, the advancement of new technology such as the Fifth Generation (5G) technology with countless merits and demerits, especially for hackers and malicious users [5] who are interested in inflicting mayhem to private and public entities. Even developed nations in today's cyberspace are vulnerable to cyber threats, as evidenced in the 2016 U.S general elections, and the WANA CRY disaster that stroked some part of Europe and Russia. It was made possible due to

the advanced hacking software available on the internet and performed by highly skilled cybercriminals targeting governments and financial institutions worldwide. The probable intrusion done by hackers will potentially lead to security threats. Notably, it hinders the economic development of nations, which Sierra Leone is not an exception. Most developing nations have embraced the internet but failed to protect their cyberspace. This is as a result of poor knowledge in cyberspace technology.

Unfortunately, the utilization of cybercrime activities without providing solutions to the challenges will render a country's defense system vulnerable to internal and external threats causing mayhem to the natural resources of any nation. Therefore, this research is aimed at providing solutions that will possibly reduce those cyber threats and risks, as cyberspace is becoming hard to monitor and control.

Protecting a nation's cyber ecosystem is paramount for national security. Internet is a borderless network that connects all the networks and enables malicious online users to inflict endless mayhems [6,5] to nations through computer technology, making them unidentified through the virtual private networks (VPNs). Internet protection demands the global communities to collaboratively map effective cybersecurity guidelines and policies for a safer and secure cyber ecosystem.

Several government security agencies have persistently developed and implement strict policies relating to internet utilization. The United Nations produced a resolution mandating the International Telecommunications Union (ITU), a UN agency that leads the effort to spread a culture of cybersecurity. The ITU implemented the conventional conceptualization framework on how to challenge the uncertainty caused by cybersecurity. This means a universal principle on how to respond to those cyber-attacks should be initiated, and all nations should adopt and follow A Johannesburg resolution recommends that all nations should legislate a national certification to fight cybersecurity-related issues.

The Johannesburg resolution is strategically based on how industrialized nations react to these threats, though the U.S perceived the resolution as not explicitly defined. The study uses results from the questionnaire distributed to the two research institutions: ONS and the cybercrime unit at the CID.

Motivation

Criminals who hijack computers [6,5], cell phones, computing and communication gadgets, with viruses and malware perform cybercrimes. The smartphone is a platform where people are hacked and sensitive data stole [7]. Norton's annual cybercrime report states that in the past three years more than 5.4 million internet users were under attack intentionally or unintentionally by online fraudsters. Hackers create security threats by creating various security vulnerabilities that compromise online users' data. By downloading malicious applications or links discloses substantial details on the user's activities to a cybercriminal [8].

Cybercriminals target computing devices to gain online access to user's information through computers, e-mails, and social media platforms. It is estimated that the human population will face numerous cyber-attacks shortly, particularly via smartphones according to the research forecast. Mobile applications are software developed to be used in smartphones, tablets and other ubiquitous mobile gadgets to improve and make the use of technology more appealing. Mobile applications serve as a cutting edge for cybercrimes globally. The applicability and usage of mobile gadgets exponentially upsurge annually, and its users will likely increase to more than half of the human population. The increase in mobile gadget usage with little knowledge of security parameters enables hackers to steal valuable information leading to millions of U.S dollars annually.

Personal computer apps store serves as a platform for downloading software, while mobile apps are programs downloaded onto mobile devices. Downloading from an unauthorized source often leads to downloading malware and viruses. Mischievous software such as malware is the state-of-the-art tool utilized by cybercriminals. Downloading apps from un-trusted sites may pose serious security concerns.

General Analysis

Cyber Security, an ingredient of the internet revolution where users are liable to get either exploited sources or to be exploited by cybercriminals. Cybersecurity comprises of several key technologies, processes, and practices executed to render computer networks, software, and sensitive data safer from potential attacks. It can also be viewed as a process that detects and prevents unauthorized access to people's data. Data invaders known as intruders or hackers are people with malicious intentions, and they should be prevented from illegally-gaining access to people's data.

The process of detecting whether an unauthorized entity has breached your computer networks or systems is a good security practice. Therefore, several governments around the world have increased financial spending on defensive purpose including security intelligence. For instance, the U.S, China, Saudi Arabia, Russia, and India spent about $610.0 billion, $228.0 billion, $69.4 billion, $66.3 billion and $63.9 billion U.S dollars respectively on military defense, as stated by the Stockholm International Peace Research Institute (SIPRI) in 2017[9,10], and it was projected to double in 2018. Furthermore, most industrialized nations have increased their military budgets; the U.S, the People's Republic of China, Russia, France, the U.K, and some African countries: Nigeria, Ghana, Egypt, and South Africa.

Moreover, securing online activities and processes demand effective and supervisory role to protect the information system as a strategic factor of cybersecurity scheme:

- Application security.
- Information security.
- Network security.
- Disaster recovery.

Application security refers to the systematic use of software and hardware to protect computer applications from internal and external security threats. Security patches are embedded into applications to mitigate unauthorized intrusion aimed to disrupt, steal, or delete sensitive data.

Information security is attributed to securing sensitive data and information systems from unauthorized access, use, interference, manipulation, inspection, recording or destruction. According to [11] provided an effective scheme for confidentiality, integrity, and availability. Confidentiality, ownership, integrity, validity, availability, and service are known as the six atomic components of information systems. Networking security has been the fundamental component of the internet infrastructure, usually supervised by a network administrator or system administrator who continuously implements standard security procedures daily.

A disaster recovery plan (DRP), is a systematic procedure on how an institution manages disasters. DRP encompasses business processes and continuity of its systems; including meaningful practices that prevent and make stakeholders proactive, securing organizational continuity than being reactive. Communication devices, systems, and networks are becoming more intricate, and perhaps inflicting undesirable effects on societies and individuals. As a result, preventive procedures are becoming more difficult [12].

Problem statement

Informatization, big data, cloud computing, and IoT are the main trends in global cyberspace. To these directions, security and privacy become a major concern. The global communities, from individual organizations to government entities, have experienced massive cyber-attacks. These attacks have adverse effects economically and incapacitate organizational functionality. A trained and qualified computer programmer, who exploits a vulnerability in an organizational computing platform, usually carries out cyber-attacks.

Although there are few departments such as the SSD and ONS who temporarily handle cyber-related crimes, Sierra Leone lacks the necessary legislation to fully handle such issues. Another dilemma is the country's lack of much-qualified cybercrime and cybersecurity analysts. The digitalization of telecommunication infrastructure interconnectivity creates more security risk than the analog systems. National and individual institutions should be in place to provide solutions to the numerous cyber threats nationally and internationally. Sierra Leone state security forces both military and the police force should be able to protect the country from any cyber-related crimes without compromising national security.

Aim of the Thesis

The key goal of the study is to examine the role of cybersecurity to minimize cybercrime in postwar Sierra Leone. The advent of the Fourth Generation (4G) technologies in early 2019 in Sierra Leone has positive impacts. Weak communication infrastructure in Sierra Leone has attracted several internet fraudsters to actively operate within the confines of Sierra Leone. Several financial organizations and government agencies have been attacked lately. Privacy and data security are key factors to maintain and protect the cyber ecosystem.

Effective cybersecurity legislation will reduce cybercrime rates in Sierra Leone. Several institutions and individuals have been affected by cyber-attacks, but have no knowledge of the perpetrators and how the attack was carried out. For instance, many people, commonly politicians, have had their characters tarnished on social media platforms without the cybercriminals apprehended by the security forces. Mobile theft is another serious issue happening daily. Notwithstanding, burglars normally surveillance social media [13,14], like Facebook, and other social media platforms for people who publicly disclose their holidays to break into their houses and steal valuable items while they are away.

The study therefore only included the SSD of the Sierra Leone Police Criminal Investigation Department, and the ONS to monitor cybercriminals and, afterward reduce or eliminate cybercrimes in the country.

Objectives of the Thesis

The following are the key objectives of this study:

- To investigate the challenges and risks associated with cybercrime in Sierra Leone.
- To provide public awareness of and a research resource on cybercrime-related activities.
- To clarify the significance of cybersecurity, and spot best standards in protecting Sierra Leone cyberspace.
- To recommend the best security practices and enhance the ICT infrastructure.

Scope of the Thesis

The scope of the research is limited to Sierra Leone, which is founded on the West coast of Africa. The study investigates the role of cybercrime in mitigating the online crime rate in postwar Sierra Leone and provides solutions to the growing threat posed by online criminals. Cybercrime is a terminology that describes the act of using cyberspace to steal or cause mayhem to people, organizations and/or governments via computer technology. It is mostly done via the internet where attackers invade a computing system to steal sensitive data, corrupt systems by viruses' infections, botnets, and various email scams [15].

Research questions

The key feature of the research is to minimize cybercrime in postwar Sierra Leone and to recommend effective solutions to the government for prompt actions. To achieve this goal, the following questions will guide the research:

- Cybersecurity and its significance in securing the nations' data from cybercriminals.

Cyberspace is naturally free for everyone, raising a series of security concerns for individual nations or entities. Digitalization has engulfed all nations and it is the common trend to achieve informatization in all aspects of human activities. Another major issue is the use of IoT. Internet connects all other networks globally, and IoT goes beyond the use of the internet, involving all electronic and electrical gadgets that are connected to the internet. Several cyber threats are inflicted on nations and individual organizations by cybercriminals and have made nations to be inactive readiness to protect potential security risks and cybercrime [16]. Cybercrime refers to internet crime perpetrated by either state actors or individuals against another state or individual, either for political or other motives [17].

- The Challenges and vulnerabilities that exist about cybercrime in postwar Sierra Leone.

Sierra Leone has experienced multiple security challenges and threats in cyberspace. The lack of proper internet connectivity is a major problem coupled with a lack of sufficient energy to power computing devices. Approximately, less than half of the country's population of the 7.396 million use the internet. Furthermore, the lack of computer knowledge and internet usage poses great threats to both government and individual organizations in the country.

Normally, three distinctive security risks are identified by internet users: 1) Data stolen from individual entities might be used for different purposes by the cybercrime, 2) manipulation of misused credentials might harm an organization functionality, and 3) hijackers normally take charge of peoples' online activities based on the stolen resources[18].

Limitations of the thesis

The author presented the research in a proper order based on a series of interviews conducted, and questionnaires were distributed among the respondents of the two researched institutions. It was hard to compare and interpret the results obtained from the qualitative method. The researcher was faced with difficulty in transportation to the targeted institutions, due to traffic congestion in the city center. There were slight similarities between ONS and the cybercrime unit in how they secure their organizational assets, such as digital systems, networks, databases, printers, workstations, ATMs, but operate differently. The cybercrime unit and ONS use both traditional investigative procedures and modern cyber techniques. One of the major problems with these two research institutions was the level of understanding and IT qualifications among top state security personnel. Most have little knowledge of computer technologies and their related disciples. The reluctance in providing detail information to the researcher

was another difficulty. It was difficult to gather detailed information, as most security personnel referred to it as a national security issue, and therefore, should be handled and research by security personnel, rather than civilian. The ONS and the cybercrime unit at CID staff will not admit to any vulnerability in their systems, fearing that, it might be exposed to the public. In most situations, they were not willing to share sensitive state security issues. A broader approach was used in conducting the research, because of the constraints. However, a mismatch between answers to the interview questions, and comparison models, as a result of a semi-structured interview, and the level of secrecy applied in state security domains.

Thesis structure

The thesis is partitioned into eight (8) chapters. Chapter 1 narrated the general background to the study. Chapter 2 reviews the literature of pertinent literature to the research. Chapter 3 presents the thesis statement. Chapter 4 describes the threats and challenges faced by cybersecurity. Chapter 5 discusses the digital risk assessment in the 21st century. Chapter 6 presents the vulnerabilities and the way forwards in a cyber-ecosystem. Chapter 7 discusses the findings and results of the research. Chapter 8 presents conclusions and recommendations.

Chapter 2
Literature Review

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

***Corresponding author:** Ibrahim Abdulai Sawaneh, Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

Introduction

This chapter presents the relevant works of literature on the researched topic. Several kinds of literature were used to thoroughly examine the challenges and risks associated with cybercrime in postwar Sierra Leone.

Literature Review

The globe has seen a series of cyber-related issues posing countless security threats and challenges in Sierra Leone [19]. The research is aimed at key security parameters encountered in the last two decades. Initially, the security issue was manned by the military concentrating only on warfare between 1945 to the cold period. Buzan and Hansen [20] discussed more on security issues than on defense or war, or war as its main objective, a conceptual shift leading to a broader perceptive of political issues, including the importance of societal cohesion and the relationship between military and non- military threats and vulnerabilities" National security is a strategic scheme used to protect territorial integrity of any nation. This implies a security issue should be state-centric. Several cyber-attacks have occurred in the last decade such as sighted in the Arabic Spring uprising in 2011, the Ransomware attacks, and DiskCoder.C in 2017 caused a major financial crisis in the world. Millions of internet subscribers had their personal information hacked in an unprecedented manner, leading to confrontations among countries and institutions. These attacks alarmed critical security issues, and further exposed security flaws in the surviving security infrastructures.

For instance, the Equifax breached in the U.S that affected several adult populations. The HBO hacked that compromised actor's roles in scripting and episodes of the Game of Thrones Series. The attack on Yahoo subscribers' database exposing personal data including names, date of birth, email addresses, passwords, and sometimes security questions and answers. A threat linking to the WPA2 encryption system, KRACK was discovered, which may compromise the security of Wi-Fi connections. The advances in modern technologies have made cybercrime possible, with several software and tutorials available on the internet categorically stating the steps on how to hack online users.

Development of cyber security infrastructure policies in sierra leone

As the world faced continuous threats more especially as we are gradually again heading towards the Cold War period similar to that of the 1980s and 1990s. The 9/11 attacks in the U.S, the 2016 melding into U.S elections, the 2017 ransomware attacks, the current trade war between the two financial powers of the globe (U.S and China), the alleged state-sponsored killing of Jamal Khashoggi by Saudi Arabia in Istanbul Turkey in early October of 2018, the South China Sea tension, the annexation of Ukraine Crimea region by Russia, and the Yenga conflict between Sierra Leone and Guinea. Due to weak ICT infrastructure, inexperienced cybersecurity professionals, weak internet and lack of energy supply to the countryside made it difficult for policymakers to successively fight cybercrimes.

The "Cold War" era granted NATO to provide all-out military power to defend European countries and their allies, and to maintain a "balance of force" by maintaining stability and security [21], the Proliferation of Weapons of Mass Destruction (WMD) executed by NATO, the EU crisis management operations under the "Berlin-Plus" arrangement [22] and supporting the general ad-hoc security processes [23]. The security concept of NATO was further enhanced when the North Atlantic Council proclaimed that terrorism could affect the security interests of NATO members, and Article 5 was invoked after the 9/11 attacks [21]. Article 5 indicated any attacks against member states are an attack to all.

Though the above description is not applicable in the present scenario, the African Union (AU) has initiated an alike mechanism to safeguard individual member states against cyber-attack. It is key on individual states in African to design a strong mechanism that counters cyber threats among member states. Cyber is defined as a digital podium that involves the formation of data, storage facility, and shared in the cyber ecosystem. It includes both the virtual and physical ecosystem that allows the virtual data to flow [24]. The more communication gadgets are linked together, the more cyber threats surfaced daily, technological innovations and several security breaches have broadened the concept of "cyber" to practically anything linked to the digital and electronic systems. Sierra Leone is faced with a huge task on how to secure its cyberspace by finding a common ground that will attract potential investors, playing as cybersecurity has gained importance in societal developmental initiatives, conflict resolutions, security, and economic enhancement. Therefore, the country must deal with its emerging cybersecurity problems.

Global connectivity and the cyberspace

The continuous advancement in telecommunications and mobile technologies has increased the chances of hackers to invade people's security and privacy globally. This is so because Sierra Leone lacks the basic fundamental cybersecurity infrastructure and policy that are yet to be enacted in the House of Sierra Leone Parliament according to the information and telecommunications Minister, Mr. Mohamed Rado Swaray in a recently held conference in Addis Ababa Ethiopia in 2018. This means that urgent attention is requiring protecting security and privacy in the 21st-century cyberspace. Cyberspace has no boundary and goes beyond the internet and IoT. Accordingly to Richard Clarke, cyberspace constitutes of the internet, computer networks and everything they interact

with, such as transactional networks used in online transactions, networks deployed in controlled panels that operate pumps and generators[25].

A typical example of global connectivity and the cyberspace is evident from the fact that today's generation exhibits interconnectivity, such as having a well-planned schedules on their Smartphone: an alarm to wake them up, checking of bank account, using GPS to drive to work, checking of health status via mobile devices, and host of other things. All human activities are now becoming smart as evident in smart devices, smart homes, smart cities, smart surveillance, VARNET, and smart transportation systems.

The above narrations suggest that we are hyper-connected and goes beyond the IoT. The IoT ensures that our devices are interconnected and keeps track of our daily activities at home and in the workplace. The Center for Strategic and International Studies indicated that IoT attributes an IP address, onboard computing power, and must have networking connectivity, which is normally a wireless connection. They go beyond our normal daily routines, such as industrial gadgets that aid our daily routines including inventory control, and planning shipment and delivery as stated in the CSIS report. The document indicated how IoT gadgets are defenseless to hacking. It noted that several of these gadgets lack computing power in performing security tasks just like a traditional computer[26]. A new global connectivity era has emerged and more importantly, the introduction of 5G in the telecommunication industries.

A financial transaction will be processed online within a single click, and feedbacks will be received from the recipient. Networks instantly store the host information. E-medical and e-diagnosis are now possible. To crown, it all, human nowadays hardily go without evolving the cyberspace. Connectivity moves a nation forward, ensuring that each nation interacts with each other's, ranging from governmental, diplomatic, education, science and technology, trade, economics, and host of other issues.

The emergence of social media networking sites has prompt online criminals to be actively engaged in cybercrimes in the country. Unfortunately, most internet subscribers in Sierra Leone lack basic security and computer skills to protect their individual information. According to the U.S Census Bureau 2016, Facebook had 1.5 billion active users every month globally, and Instagram having more than 400 million active users monthly. In July 2018, the U.S. Census Bureau mechanized a vigorous cybersecurity platform to protect the nation's information. They integrated best industry practices and follow Federal IT security standards for encrypting data in transmission. The Bureau endorsed the two-factor authentication methods for all data usability.

With everyone connected in the global village, the majority of Americans, Europeans, and few Africans relay on online and electronic transactions, including credit and debit cards for their financial transactions and carry more than $50 on any given day[27].

Therefore, Sierra Leone as a nation should enact strong cybersecurity legislation to protect the nations' information. Currently, there is no such law(s) relating to cybersecurity and information security in the country. The Honorable Minister of information and telecommunications, Mr. Mohamed Rado Swaray in October 2018 in Addis Ababa reiterated that his government will work with the Europeans to draft strong policies on cybersecurity and information security. There will be 50 billion networked electronic gadgets by late 2020[28].

Cybercrimes erode confidence and impart fear in the system. They create negative effects for individuals, corporations, business enterprises, financial bodies, and clients. The United Nations viewed cybercrime is an institution that surpasses a trillion dollars in a year in online fraud, identifies theft, and lost intellectual property. Such online crime upsets millions of people globally, as well as businesses and government entities[29].

Ensuring that the internet is secure against unauthorized access in the cyberspace is not completely guaranteed. Any device with connectivity is vulnerable on the internet. Security professionals demand continuous alertness as cyber threats are on the increase. Any challengers can easily get into a system, more especially an online platform. There are several techniques deployed by adversaries such as phishing, a common platform that traps online users to reveal sensitive information, most often to compromise personal data, credit card or other personal accounts. They then hijacked and steal valuable information costing millions of dollars. A major effect of phishing is a link that directs users to a malicious page that infects their computers[30].

Cyber Security Threat Evaluation Globally

The world has experienced a series of cybersecurity threats in the last two decades ranging from state-sponsored to private individuals costing billions of U.S dollars in damage. According to James R. Clapper, Director of the U.S National Intelligence testified to the U.S Congress in 2016 about the worldwide threat assessment of U.S. intelligence, emphasized the level of cyber threats faced by his department. Clapper stated that the "consequences of innovation and increased reliance on information technology in the next few years on both our society's way of life in general and how we in the intelligence community specifically perform our mission will probably be far greater in scope and impact than ever."

The spontaneous "assertiveness" in the alleged cyber interferences by Russian against the U.S, was emphasized by Clapper in the U.S Congress. New security threats relating to cyber threats from North Korea, Iran, and non-state actors, are in the increase according to Clapper. Cyber in its self is different from conventional warfare, where the state immediately responds to an attack. Clapper indicated that opponents are "emboldened" and "undeterred" in steering reconnaissance, espionage, and even attacks in the cyber ecosystem because of the "relatively low costs of entry, the apparent payoff, and the lack of substantial consequences." Russia and China are among those who "view offensive cyber capabilities as an important geostrategic tool and will almost certainly remain developing them while simultaneously deliberating alternative schemes to limit such use,"[31].

The United Nations should enact bills to guides and protects individual member states regarding cyber military operations, to preserve global peace and security, akin to rules of engagement in traditional warfare, such as stopping attacks on protected network sites (hospitals, banks, immigrations, state security agencies). President Obama hosted his Chinese counterpart, President Xi Jingping for an official visit in 2015, with the two world leaders agreeing to deepen collaboration in cybersecurity[32].

There is an imminent security threat where a conflict may emerge that will have a significant impact on which enemies deploy cyber warfare against another nation. According to Col. Carmine Cicalese, a cyber-professional with Army Operations Center, G-3/5/7, stated how online criminals continuously scout for weaknesses in the army's networks, and how those attacks are on the increase. He explained that they rely on networks for several critical tasks, manning sophisticated weapon systems to performing wartime operations. An enemy who compromises the network could compromise the mission. "That threat is out there daily," he said. "We're reliant on our networks. We're completely dependent on our communication systems, so that's vulnerability and a non-lethal vulnerability, at that, where they could affect." In the next war, "someone's screens are going to go blank," he said. We do not want them to be ours [33]. This can be evident from the ongoing talks between the U.S and China relating to the stealing of trade secrets and other issues, and also between the U.S and North Korea concerning the denuclearization of the Korea Peninsula.

Cyber Activities in our Day-to-Day Activities

Sierra Leone as a nation does not have any technology that will support cyberinfrastructures in military operations. There are no laws relating to cybercrime or electronic crime and/or cybersecurity in operation since the country gained independence in 1961. During the bloody civil war that ravaged the country (1991 - 2002), the country evidences many cyber-attacks, though not on a large scale. Collaborators of the Revolutionary United Front (RUF) communicate sensitive information to the rebel group, including military secrets to the RUF. With such information, the RUF mounts an attack on the military bases and territories that resulted in large civilian and military causalities. Most nations around the world are working on strategic policies that will defend their countries from an eminent cyber-attack from adversaries.

Furthermore, after the civil war was declared over, many telecommunication companies established their networks in the country. This was an opportunity that supposed to make communication easier as compared to the outdated communication channel. But with the advent of faster internet (4G) in Sierra Leone, augment the use of social media and electronic banking systems in the country. Unfortunately, most people in the country especially the youth are not computer literates and also lack the expertise on how one should protect their personal information when connected to the internet. This is more important because most banks in the country have weak infrastructures to tackle large scale cyber-attack.

Cyber Attack in Picture

Analyzing cyber threats and vulnerabilities in developing countries is paramount. This is because most lack the expertise in legislating and protecting state secrets and individual's or company's information from unauthorized access and use by third parties. This was proven in the 2014 crippling attacks by North Korea against Sony Pictures Entertainment. It was a vengeance game, "the interview," a comedy movie where few American reporters hired to assassinate the North Korea leader, Kim Jong-un.

The action angered Pyongyang and North Korea supposedly took revenge by launching cyber-attacks that endangered Sony workers and the public, stole and destroy data, and publicized trade secrets, and disseminate sensitive information to the internet [31]. The most devastating aspect of these attacks was that several private corporations were unable to detect and prevent it from happening according to Joseph Demarest of the FIB's cyber division in the U.S. According to him at a Senate hearing, stated that there is a possibility of a malware likely to challenge even a state government [34]. An investigative report made by Peter Elkind in Fortune proved that the malware wiped out thousands of data computers and servers, and overwrite the computers' data with a special deleting algorithm, leaving the computers useless. Also, hackers released thousands of confidential information: social security numbers (SSN) of thousands of employees, uncompleted film scripts and unreleased films [32].

The online enemies of the U.S threatened with 9/11-style assaults on theater-goers. They warned "how bitter fate those who seek fun in terror should be doomed to … The globe will be full of fear. Remember the 9/11 in 2001. Peterson recommended Americans to distance themselves from crowded places. Sony initially releases the movie, but finally released it too few theaters [35].

The company was in a terrible shock from the incident as the federal government was outraged. Responding to the attack, the Obama administration struck new sanctions against North Korea for its provocative action, destabilization, and oppressive activities, and policies mainly its destructive and intimidating cyber-attack on Sony Pictures

Entertainment," [36]. Furthermore, the "Wanna Cry" cyber-attacks that affected most European countries, the U.S, China and Russia in 2017. These attacks were also linked to the same North Korean hackers.

Ethical hacking as a turning point in cyberspace

The presence of tough adversaries in cyberspace, the Minister of Information and Communications, Mr. Mohamed Rado Swaray urges Parliament to legislate laws that tackle cybercrimes and its related components. He requested that they should liaise with countries with adequate knowledge on best practices on hacking and cyber technologies to help Sierra Leone build its cyber laws. The information ministry every year should organize "hacker's day" in Sierra Leone to identify talented and skilled young hackers, who will be employed to defend the various ministries' online activities. This helps minimize cybercrime rate, and also create awareness among internet users in the country. If the government implements such a conference for cyber experts, strong cyber laws will be enacted to combat cybercrime and cyber-related issues in the country.

For instance, the Department of Defense launched a cyber-bug bounty program in 2016, "Hack the Pentagon" program, controlled and limited in duration, according to the Pentagon. This ensures that "white hat" hackers are gifted with skills that search for possible vulnerabilities in the Department of Defense websites, and grant them "monetary awards and other recognition" for their imminent discoveries. "Inviting professional and patriotic hackers to explore vulnerabilities in state critical structures is needed to meet the test of difficult situations. Carter was confident to attests that technological innovations will surely strengthen digital defense and ultimately enhance the national security" [37].

Industries and corporations around the globe heavily depend on "ethical" hackers to point out vulnerabilities in their systems. Private companies having bug bounty programs are Apple, Facebook, Microsoft, Samsung, PayPal, and many other apps. Crowd-sourcing allows hackers to exploit vulnerabilities within a system by adhering to the rules of the game, with diverse approaches and skills employed to help patch the company's weaknesses is possible through crowd-sourcing [38]. Recently, Facebook claimed to have paid millions of U.S dollars to hundreds of people around the world in its bug bounty program in 2011. Highlighting the increase in innovations in technology globally, in 2015 alone, Facebook received many submissions (13,000) from more than 5,500 people in 127 countries[39].

Cybercrime statistics

The increase in technological innovations among nations in 2019 requires proactive measures to tackle cyber-related crimes. This is as a result of the Cybersecurity breaches survey conducted in 2018, around 43% of global business was affected by a cybersecurity breach. Some states in the U.S, such as California lost more than $214 million U.S dollars through cybercrime alone.

Virtual Private Network (VPN), a tool used to protect people's privacy online in the last few months is utilized by most internet users either private or public organizations globally. Unfortunately, Sierra Leone as an emerging nation with low technological expertise and innovations lacks the necessary platform to tackle large scale cyber-attacks. Even though with the awareness associated with the risk of clicking a link, or opening an unidentified email, the number shows that cybercrimes and attacks are on the increase.

McAfee's Economic Impact of Cybercrime

An assessment was done by McAfee's Economic Impact of Cybercrime in February 2018 indicting that cybercriminals were at a faster pace. The scale of malicious activity on the

internet is quite surprising. The figure is on the increase every year. Electronic criminals are continuously exploring new schemes that exploit online users. Bitcoin as a payment and transfer method to /from criminals is untraceable. About 780,000 records were lost per day in 2017, according to McAfee's Economic Impact of cyber Crime in 2018.

Malicious Mobile Apps

Symantec's Internet Security Threat Report shows that lifestyle apps are the main targets. Most of these apps expose mobile phone numbers. Moreover, sensitive information such as device location is made accessible. It would be impossible to monitor or check each of these apps for vulnerability issues. It is more so easy access for cybercriminals to lunch cyber-attacks. In the first quarter of 2018, Google play had over 3.8 million apps on their store.

Mobile phone

Globally, the mobile phone is the order of the day in attaining effective communications and performing online transactions, and so do fraudsters who are involved in the process. About 60% of fraud comes from mobile devices; out of that number, only 80% of these frauds come from mobile applications. Once a cybercriminal has access to your mobile device, the fraudster can easily access your mobile banking apps and initiate multiple levels of cybercrime. Fraudulent transactions double the value of real transactions.

Smart home attacks

Almost all smart home devices are connected to an external network. Utilizing a router with poor security features will lead to a possible cyber-attack. With smart home devices becoming more prevailed, criminals are exploring new schemes to exploit vulnerabilities in mobile apps globally. The U.S, U.K, & China are more vulnerable to smart home attacks. According to Trend Micro, the U.S accounts for 28% of smart home device attacks. The U.K and China followed by 7% each.

Cybercrime and the future

According to the 2017 Official Annual Cybercrime Report, it forecasts that cybercrime will cost about $ 6 trillion U.S dollars yearly. It indicated that about $ 3 trillion of such attacks took place in 2015. Cybercrime is a lucrative business that seems to be more profitable than the illegal global drug trade.

Phishing

Verizon's 2018 Data Breach Investigation Report suggested that about one - third of all emails are affected by a phishing attack. The new scheme is now adopted which is quite different from the traditional phishing attack. For instance, some emails from Banks, Apple, PayPal, Microsoft, TaoBao, Huawei and host of others requesting sensitive information. Most are phishing attacks exploiting potential email victims. Most people receive emails daily, and about 12% click on the links/attachments contained within them.

Cyber security advice

Cyber Security Breaches Survey conducted in 2017 indicated that most businesses in the U.K are aware of cyber issues. However, the survey also indicated that a greater percentage of businesses are seeking advice as to how they can potentially protect their companies/corporations from cyber threats. The survey further illustrated that about 79% of medium firms sought advice whereas only 50% of the micro firms responded to such advice.

Passwords

Passwords are gradually fading out, due to data encryption and two-factor authentication schemes. According to Cyber Security Media, they are not. It is predicted that 300 billion passwords will be used by 2020. That takes into account humans and machines. This requires cybersecurity protection. It is estimated that about 300 billion potential threats worldwide.

Personal data sells for as little as $0.20

Have you ever imagined how much your data worth? Some people can sell for as little as $ 0.20, up to $ 15. Relevant information concerning our credit cards and personal accounts can be accessed and purchased much more easily than you might think. The value of information is dependent on the type of details included. For example, credit card details are more valuable than other information. As well as this, it's also dependent on how easy it would be to resell the information. If it's too difficult, the value of personal data decreases.

Hackers deployed encryption method to defraud

Today's hackers most often utilized encryption as a tool to hack into personal and company records. Encryption involves encoding a message, information, or program. It only permits legitimate users to access it. For instance, a document that may be readable in normal circumstances would appear completely not readable when encrypted. To access encrypted information, it must be decoded first. Hackers are of course aware of how best to hide their tracks. 90% of them use encrypted traffic to disguise what they're doing. If we as users, used encryption to the same level, it would be much more difficult for cybercrime to take place.

Adware attacks

It has been suggested that about 75% of companies are affected by adware attack, according to "Cisco 2017 Annual Cyber Security Report" Adware in itself is a nuisance, but it can also facilitate further malware attacks. Adware most often appears as adverts, prompting internet users to click on its link. Whether you're using your device on or off the internet, adverts can be displayed. Often if you're trying to perform an internet search, the results will direct you to other websites or marketing pop-ups to obtain your data.

Poor file protection

About 21% of files are not protected, according to Varonis's 2018 Global Data Risk Report. Roughly 6.2 billion files were processed, and they include credit card details, immigration records, healthcare records and host of other relevant records, and 21% of these records were accessible for global access. Moreover, 41% of companies' sensitive records were compromised.

An alarming trend: The ransomware attack

Cyber professionals and individual nations around the world are proactively informing internet users about another growing trend in cybersphere; that is, hackers are using ransomware to squeeze money from users. Normally, hackers penetrate a network, computer system, Smartphone "captive," until the owner pays a ransom before unlocking the system. The targeted victims normally pay in a hard-to-trace cyber currency called bitcoins [40]. It is stated by the FBI that anyone can be targeted including individuals and government agencies.

Hollywood Presbyterian Medical Center in Los Angeles suffered a similar attack in February 2016. The hospital authorities indicated that the cyber-attack did not affect the

distribution and quality of healthcare records [41]. However, several people informed the local news channel that they were concerned about the hack. The chief executive officer of the medical center Allen Stefanek, report on NBC in Los Angeles that investigators indicated that the attack seemed to be at random [42].

About 17,000U.S dollars was paid in bitcoins according to Stefanek. He further suggested that the malware lock their systems by encrypting the company and demand ransom to get the decryption key. The center then paid the ransom to restore normal operations [41]. Unfortunately; the Los Angeles County Department of Health Services was also a victim of the ransomware attack, blocking all its data. The department was clever enough to isolate the affected gadgets and refused to pay the ransom as stated by the Los Angeles Times. A South Carolina school system in 2016 paid online criminals about $ 8,600 U.S dollars to have access to its system [43].

The amount extracted from individuals in a single ransomware attack is normally in the range of thousands of dollars as quoted by the FBI. Users can be easily infected by clicking on fake sites and links, email scams, adware, or download programs infected with malware and viruses. The ransomware highlights another alarming situation in the evolving cyber realm, suggesting how vulnerable we are, and how cybercriminals are determined to exploit and victimize their victim, whether a government institution, healthcare system, educational institution, financial institution or individual.

Threats from Nation-States

The United States and other nations are strategically worrisome about the rapid increase of state and non-state actors with cyber capability or who are seeking methods to hack into critical infrastructures. Russia, China, North Korea, and Iran make the list of nations the U.S is concerned about, according to U.S officials.

At Fordham University, Clapper informed lawmakers and students about Russia's technical and sophisticated human capabilities in its cyber arsenal. If the U.S and Russia were entangled in a cyber-conflict, "some U.S critical infrastructures will be exposed to high risk." The risk posed by Russian cybercriminals is more advanced as compared to those coming from China, North Korea or Iran.

Iran and North Korea in the past have launched cyber-attacks against U.S. networks and indicated that China is driven on stealing business and technical secrets according to Clapper. China is "cleaning us out" and "robbing our industrial base blind" through loopholes that can be simply solved with a patch. "We know we're thought to be doing those basic things, and yet we don't do them," [44].

A trade war between the U.S and China worth Trillion of dollars has been going since 2018. Presently, the two parties expect to solve their indifference in trade talks at Washington D.C in the United States by 31st March 2019. This was as a result of the tariff imposed by the U.S and China in returns imposed similar tariff. The U.S accused Beijing of stealing sensitive trade and technological secrets. The U.S also imposed a series of tariffs against the European Union, Canada, India, Japan, Mexico, and other nations.

The Mobile World Congress held in Barcelona in March 2019, a Huawei Mate X foldable phone with 5G technology was unveiled with bigger and better functionality as compared to Samsung folded Galaxy Smartphone unveiled a few days earlier. The U.S officials went to Barcelona to persuade their allies that Huawei is controlled by the Chinese Communist Party, and they should not be trusted by telecommunications and mobile companies to provide equipment for their new 5G networks. The Europeans raised similar concerns but other nations have gone ahead to allow Huawei to provide equipment for the construction of 5G networks.

The consensus should be made for all providers, including U.S, Russia, China, U.K, Canada, the Five Eyes and other nations should be compelled to greater scrutiny before 5G networks are embedded into critical infrastructures. A 5G sensor technology was installed across a water system to aid in identifying water pressure and enhances efficiency by locating leakages. A team from U.K's University of Surrey revealed a 5G-enabled McLaren sports car that could receive a live broadcast on other cars and threats from sensors mounted on the roads.

The inspector general at OPM had talked about the vulnerabilities as quoted by "The New York Times". He noted that the mystery is not how they got cleaned by the Chinese but what took them long. Unfortunately, the chief information officer Donna Seymour quit before the planned hearing to the House Committee on Oversight and Government Reform. The American people were never able to hear from those who were controlling the systems at that time, and probably clarify what went wrong. The testimony could have certainly answered some of the questions asked from those who were affected by the hack, but also provide understandings to government and non-governmental organizations on how to avoid such a breach in the future by moving forward [45].

Furthermore, postmaster general Patrick Donahoe highlighted that it is "an unfortunate situation these days that almost all institutions linked to the internet are constantly under cyber-attacks" [46]. China was allegedly behind the cyber-attacks involving the stealing of design plans for more than twenty chief weapons systems including the F - 35 Joint Strike Fighter [46] as reported by a Washington Post. China denied that allegedly copycat aircraft, the J-31 fighter [47]. CNN report revealed documents leaked by former NSA worker Edward Snowden suggesting that the U.S. government consider China stealing "several terabytes of data" associated with the F-35 fighter jet [48].

Some members of the Chinese military officials were charged in the U.S District Court of Pennsylvania in 2014 for supposedly hacking into government files, being one of its kind involving state-sponsored actors in the U.S as stated by then-Attorney General Eric Holder. They were charged on 31 counts, including aggravated identity theft, economic espionage, and theft of trade secrets in the U.S nuclear power, metals and solar products industries. The FBI indicated that the men hacked into computer networks of six American organizations, and potentially stole trademarked data including email exchanges among workers and trade secrets for nuclear plant designs [25].

"According to James Comey Director of the FIB in the U.S, China has "blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries," [49]. The alleged hacking by China on U.S systems is on the increase according to U.S officials, though the U.S has not been able to come out with a piece of tangible evidence. Some analysts viewed it as a power struggle between the two world's largest economies. I doubt what will happy with the personal data of millions of government employees and internet users globally.

Russia was taught to have launched a "Trojan Horse" attack, a malware program that penetrates computer systems and causes a devastating economic loss as cited by the Department of Homeland Security bulletin according to ABC News. Officials noted that the malware lasted for two consecutive years and unable to harm their critical systems. The news according to DHS sources thought the Russians were behind the attack hoping to gain a strategic advantage over the U.S in terms of war [50].

According to Clarke in his book, that the Georgian government was victimizing through a DDoS attack, and its website vandalized during the Georgian Russian war in 2008. A series of attacks cyber-attacks against Georgia incapacitated them not to access news to perceive what was happening during the war. Online banking transactions with the use

of credit cards and Smartphone operations were cut off, Clarke said. “The DDoS attacks originated from six different botnets via computers hijacked by hiding the criminal’s online activities and people who download hacker software from several anti-Georgia websites,” [51].

In late December 2015, power was cut off in the winter in Ukrainian, which the Ukrainian authorities accused Russia of the possible cyber-attack, according to Jose Pagliery on CNN as a measure of its conflict with Ukraine over Crimea. Mobile communications were also jammed making mobile subscribers unable to report the outage [52]. Directing the cyber-attacks against the civilian populace and infrastructure are against the universally acknowledged rules of engagement in conflict, and were extremely worrisome by the international communities.

Russia allegedly also hacked into the State Department and White House networks. Investigators consider the cyber aggressors infiltrated the White House through a phishing attack as reported by CNN. The hackers purportedly accessed emails and the day-to-day schedule of President Obama. The information was not classified, meaning that no sensitive data were released to the public [53].

The U.S has continuously accused Iran of persistently hacking U.S firms and other international organizations of stealing critical information for at least twenty-four months [54]. Furthermore, the U.S blamed Iran for breaking into unclassified Navy computer systems in 2013. The Wall Street Journal quoted a U.S official indicating that the breach was “facilitated by weaknesses that were revealed and exploited in older systems and network architecture.” The contract awarded to Hewlett-Packard Company for the database fails to include security features, and so the security features were not often maintained. This provided an added advantage for hackers to penetrate a system, and then cause disaster as cited by The Wall Street Journal. The investigation concluded that no confidential information or emails were breached. This intrusion was first of its kind by Iran authorities broken into U.S. military networks on U.S soil [55]. Furthermore, the Iranian cybercriminals were assumed to have gained control of a dam in Rye, New York, as quoted by The Wall Street Journal [56].

The Bureau 121 unit comprising of highly trained cyber professionals in North Korea is the most oppressive hacking group according to one escapee who said he trained with them before fleeing the isolated nation. Detective Jang Se-Yul indicated that there about 1,800 hackers in the unit according to an interview with Reuter’s news agency. The hackers were carefully selected by the oppressive administration and are considered the best in the isolated nation [57].

The oppressive nation in the Korean peninsula is provocative and has launched a series of cyber-attacks against other nations in the past, according to James Clapper. Pyongyang is determined to be seen as global key players, he said. Cyber is a dominant new domain for the North Koreans, he said, noting that they “can exert maximum influence at minimum cost.” The intrusion into Sony Pictures Entertainment system displays their capabilities and recognition globally, Clapper said. “That’s why the U.S has to take precautionary measures, and If they are accorded with the global recognition at a low cost with no consequence, they’ll repeat it until we push back, and of course others will follow suit” [58].

Conclusion

It is evident in the literature review that the global community is faced with the huge task of protecting individual nations and entities against cyber-attacks. We have seen great confrontation between and / or among nations relating to cyber espionage and saboteur. The United Nations (UN) and other international bodies such as the European Union

(EU), African Union (AU), Economic Community of West African States (ECOWAS), should be proactive and united in fighting against cyber-warfare in this tense cyber era. This is because most of the nuclear nations are on the verge of creating what will be known as the “Third World War” if drastic steps are not taking to avert such a disastrous situation. A nation such as European countries, the U.S, China, and Russia are highly competing for global dominance. Furthermore, the United Nations gradually becomes weakling as the main contributors in the United States that moving towards “Capitalism”; America First Policy.

Chapter 3
Cyberspace

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

*__Corresponding author:__ Ibrahim Abdulai Sawaneh, Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

Introduction

Our world today is globally interconnected to each other through the network of networks as technologies, innovations and sciences advance. Several offices, smart cities, smart homes, government departments, smart nuclear plants, defense departments, healthcare systems, and residential gadgets are developed to enhance our wellbeing, which is interconnected to each other. These interconnected gadgets are increasing day-to-day. Such areas including to name few; CCTV surveillance cameras, smart applications used in the smart city for aiding users to locate vacant parking slots, and in healthcare applications to monitor patients' health status.

Furthermore, most countries around the globe spent a huge sum of money on technological research, all for self-defense, power, wealth and meeting the basic needs of their states. With all these advancements, the internet plays a vital role in establishing solid and efficient systems; such as a nation's defense system, healthcare system, e-commerce, e-learning, cyberspace, cyber warfare, transportation. Although such advancement has substantially enhanced people's wellbeing, yet it posed a greater risk to individuals, society, nation-state and the rest of the world. Cyber-attacks have been the norm of the day and see the nation's blaming other nations for either stealing intellectual properties, trade secrets, or hacking into sensitive government information systems. The US-China trade war is as a result of such action.

Data Reliability and Validity

Roughly, there are more than 20 billion devices interconnected globally. These devices generate huge data in various forms and are transmitted via the internet that is not 100% secure. For instance, sensitive healthcare records recorded by wearable or implanted sensors that monitor patients' health status whilst they carried out their day - to - day activities without being hospitalized, or classified state information from reaching unauthorized individual or group, which implies that "Data" is an important asset of any organization and must be treated curiously.

Other instances are the role of the internet in the manufacturing industries around the world and they deployed different types of sensors in collecting vital and secretive data. These collected data will be used to analyze the global market space and make a sound judgment. For example, "Train as Service" Azuma trains in the UK are manufactured by Hitachi. The motive is to collect sensor data online and utilize these data for maintenance [59].

Most importantly, all sensitive data collected globally should be reliable and valid, which means, it should be protected from intrusion by unauthorized users either online or offline. But, this is not as easy as the world connected gadgets cover all aspects of life. All cybercriminals target these sensitive data and cause seriously damaged either financially or for the political game.

The role of internet of things in the cyberspace

The term IoT was first proposed by Kelvin Asthon in the 1990s [60] and is referred to as internet-connected devices connected through different communication methods and channels. Gartner (N.d.) stated that the industrialized internet encompasses a physical device that monitors our surroundings and transmits the supervised information to other devices, and performs actions intelligently. Furthermore, these gadgets can transfer data and interconnect with each other. The communication paths can either be wired or a wireless medium, depending on the IoT device infrastructure. Gartner in 2017 [61] indicated that approximately 25 billion IoT gadgets will be inactive operations in 2020. However, this figure is expected to be much higher than initially expected.

Lawrence Miller in 2016 defined IoT as, a concept covering gadgets and objects linked together on different communications infrastructure. They may include computing gadgets, laptops, desktops, tablets, notebooks, and mobile devices. The communication routes of IoT devices including; Bluetooth, long-range wide area, Lora WAN, and Smartphone-based wireless transmission medium (3G, 4G, and 5G) form of transportation infrastructure. These communication routes are usually viewed as a low power protocol because normally the IoT gadgets send a small quantity of data with low to transmit rate and as well in low range. In the future, IoT gadgets will communicate with long-range infrastructure with current technologies and innovations in 5G mobile networks [62].

The Fifth Generation Computer Systems (FGCS)

The FGCS was part of the Japan Ministry of International Trade and Industry initiative in the 1980s that designed a computer with enormous parallel computing power. It was planned to design a supercomputer with high-performance capabilities that will enhance the development of future artificial intelligence. A Russian plan is known also as a fifth-generation computer (Kronos computer), which is similar to the Chinese Huawei 5G technology. 5G network is referred to as the next generation of mobile internet connectivity, with faster data download and upload speeds, broader coverage and more steady connections than earlier generations.

The globe has gone mobile as existing spectrum bands become congested, leading to network unreliability, especially when several clients tend to pool from the same services at the same time. The 5G network handles thousands of devices simultaneously with high speed ranging from smartphones to sensors, CCTV cameras to smart traffic lights and smart cities. The current 4G mobile network has a speed approximately 45Mbps (megabits per second) and communication experts believe 5G will be able to solve most of the communication barriers which might likely attain20 times faster than the current networks. Some nations have already started to roll out 5G into their networks such as China, France, U.K, and others.

Cyber Law in Sierra Leone

Several calls have been made to legislate or enact strong "Cyber Laws" in Sierra Leone over the last ten years. This is because Sierra Leone utilizes global cyberspace and is also connected to the global telecommunications infrastructure and the internet. Furthermore, there have been a series of cyber-attacks globally, in which Sierra Leone is not an exception. Therefore as a nation, the government of Sierra Leone needs to enact policies and strategies that protect its citizen's data whilst using the internet and/or GSM networks.

Cyber Laws

NATCOM has called on the government of Sierra Leone to legislate strong cyber laws or data protection act that will punish anyone found wanting of cyber-related crimes in the country.

According to Lahai, the "Information and Cyber Security Engineer" at NATCOM, they have been getting frequent complaints from the general public about cyber-related crimes which he noted is seriously affecting the general populace, and also undermines the effort of government and GSM operators in their revenue generation drive.

This has to do with the daily cyber-related crimes in cyberspace ranging from mobile phones and data theft, mobile fraud and the misuse of social networking sites including Facebook and WhatsApp according to Lahai. He also emphasized that if strong laws are not legislated to protect our cyberspace in tackling sim box fraud, it will seriously deter government effort in revenue generation drive subsequently affecting the country's socio-economic development and security of the country. He urges the government to enact and implement key strategies that lead to a safe state and attract potential investors to the country [63].

NATCOM and civil rights coalition on cyber security sensitization

NATCOM in collaboration with the Civil Rights Coalition recent conducted an awareness training workshop on cybersecurity and data protection, and how to use ICT for university students and stakeholders. The workshop aimed to address cybercrime and identify online criminals who use the internet to engage in fraudulent activities. According to the Deputy Director-General of NATCOM, Daniel Kaitibi said the commission has always been under attack because of the criminal activities of cyber-related fraudsters. He stressed that the workshop is to create awareness to the general public as many people have lost millions of U.S dollars to these internet and GSM fraudsters known locally as 419ers.

According to the coordinator of Civil Rights Coalition Alphonso Manley, cybersecurity, data protection, one-gibe fraud, sim box fraud, and money fraud have become too alarming in the country, which is why his organization is standing as an advocate to address these problems. Although we are not experts in cybersecurity and data protection, yet still awareness ranging among young people who make up the bulk of the population that uses social media is very paramount.

Updating on cybercrime unit, Thaimu Bellah Sesay from the Sierra Leone Police (SLP) recalled that the unit was established in 2009, but at that time, there were fewer crimes except for sim box fraud. He noted that cybercrimes are on the increase as a result of social networking sites, especially bank fraud, internet fraud, electronic fraud, money transfer fraud, robbery, murder, and mobile theft. He also stated that the SLP is faced with challenges in the area of cyber laws that enable them to punish cybercriminals, and they only used the Public Order Act of 1965 to prescribe minimal fines and use the 2005 NATCOM act to punish the fraudsters for sim box fraud [64].

Information ministry looks at cyber security

Mathew Shears of the Global Digital Partners in March 2019, the Information Ministry, and partners conducted a two-day conference where they discussed the draft policy on cybersecurity and give feedback on the proposed draft. The minister, Mr. Swarray urges the participants to participate in the process of validating and implementing the strategy, as well as sincerely discuss possible collaboration with civil society in actualizing the proposed strategy.

He further informs participants that the world is a digitally interconnected community with most nations completely relying on online technologies and innovations. Sierra Leone has an emerging nation that should embrace ICT and sciences to compete with the global communities, especially on cyber-security. The Minister argued the government of Sierra Leone to have a cordial relationship with nations such as U.K, Ghana, EU, Nigeria, and others because of their expertise in the field of cybersecurity and information security.

The participants of the conference were expected to suggest concrete strategies that will deliver successful cybersecurity policies. Mathew Shears of the Global Digital Partners based in the U.K and Kenneth Ado Amanfoh from Ghana were the key facilitators of the conference, and include participants from all sectors of life in the country. According to Edmond Carter working for the ISATT here in Sierra Leone, the British Government has been playing a vital role to help the government of Sierra Leone to draft sound policies in cybersecurity. He cited that “fighting cybercrime” is a joint task by all governments to security and sanity, as several organizations and governments have suffered from cyber-attacks in the last two decades.

Mathew Shear emphasizes the reason why security is vital for any nation especially developing countries with weak structures, particularly those coming from cyber threats and risks and that more key players should be involved to fight against cyber insecurity. Securing the cybersphere, according to him is good for economic, social and political standing, and indicates if a cyber-threat occurs, all sectors across the government will be affected. He stressed that cybersecurity refers to the protection of internet-connected devices including hardware, software and other connected infrastructure as the information transmitted along the paths is used by both authorized and unauthorized entities that can be used for either good or bad motives depending on the intention of the intruder [65].

Feature of the Cyberspace Environment

There are various features of the cyberspace environment, and only a few selected ones are discussed below:

Networking

A network is defined as a group of computing devices and other devices connected to exchange data. Each of the connected devices on the network can be thought of as a node; each node has a unique address. Therefore, for secure and better cyberspace, the

individual network should be well protected to prevent attackers from invading peoples' personal and government information.

Furthermore, several devices connected to a particular network under attack, possibly render the entire computing devices connected to that network vulnerable provided, they are not secured; i.e. without a firewall, anti-virus and other safety measures.

Computer platforms

A computing or digital form [66] is an environment in which a piece of software is executed. It may be hardware or an operating system (OS), even a web browser and associated application programming interfaces, or other underlying software, as long as the program code is executed with it.

Computing platforms have different abstraction levels, including computer architecture, an OS, or runtime libraries [67]. A computing platform is a stage on which a computer program can run. A platform can be seen both as a constraint on the software development process, in that different platforms provide different functionality and restrictions; and as an assistant to the development process, in that they provide low-level functionality ready-made. For example, an OS may be a platform that abstracts the underlying differences in hardware and provides a generic command for saving files or accessing the network.

Computer Virus

The following issues occur when attackers get their victims [68]:

Viruses

A computing system infected with a virus (s) should never be trusted because it has already been compromised or breached. For most sysadmins, the appropriate action is to dust off and nuke it from high orbit; meaning format and reimage the machine. Essentially, a computing system should are to be backup to prevent breakdowns in operations.

Deleted files

Proper data backup preserves critical and valuable data as most malware always targets critical data on workstations, external drives, and share networks. It will be a catastrophe to the victims more especially when irreplaceable data such as important business records, family photos or sensitive state secrets are compromised.

Encrypted files

For the last decade, ransomware has been one of the main threats faces by individual nations, organizations, and individuals. The attacker intrudes and encrypts the victims' file and they will not be able to decrypt the file until payments are made. No payment, no more data. It's known as digital extortion.

Zombie plagues

Some malware tends to transform a victims' computer into zombies and use the infected machine to launch an attack against other systems. Sometimes, they will result in colossal denial of service attacks; they might be used to break into other machines either through brute force or distributed cracking.

Rats

Rats are a tool used to steal sensitive information and/or as an espionage tool via webcams and microphones due to the backdoors created by a remote access Trojans in a computer

Cybercrime through social websites

The rapid increase in social media platforms; Facebook, WhatsApp, Twitter, LinkedIn, Myspace, Email, and others have pros and cons in the telecommunications and ICT industries. About 95% of the people who use these social media apps lack the basic knowledge of security issues, and therefore, they are vulnerable to cyber-attacks, in most cases, find it difficult to acknowledge the attack.

Furthermore, the majority of internet users in Sierra Leone can easily provide their details online, and most time, they open suspicious links especially emails. They sometimes even accept friends on Facebook, whom they do not know or not knowing that someone uses their close relatives or friend's pictures to create a fake Facebook account. Also, most Facebook users in the country displaced sensitive information on their Facebook blog, which cybercriminals use to attack them.

Cybercrime via smartphone

According to the cybercrime unit at the Criminal Investigation Department (CID), cybercrime via smartphones is on the increase (Awoko Newspaper). In late 2018, a fraudster impersonated himself to be the Speaker of the Sierra Leone Parliament and demanded high profile Sierra Leonean to send him one million Leones Orange mobile credits, but unfortunately, he was arrested and detained by the cybercrime unit at the CID headquarters. The instance of similar Smartphone frauds has been reported throughout the country especially, the congested capital city of Freetown.

Hackers

Living in a globally connected cyber environment where almost all devices are interconnected either directly or indirectly via the network of networks "the internet". Unfortunately, no system is 100% secure from a security threat, some internet users just make it easy for hackers and attackers to infiltrate into their systems. They forget that they (users) and cybercriminals use the same source (internet), where they are exploited knowingly or unknowingly. A hacker is anyone with the technical knowledge and expertise who intrudes into a system in an unauthorized manner. A security hacker is someone who uses his/her knowledge to break into a computer system. They are also known as crackers[69]. This normally results in substantial financial loss and identity theft. These hackers, crackers and or attackers deploy malicious malware in various forms to cause damage, takeaway credentials, steal valuable information, search for a systems' back door, or "use you" to make an even a bigger gain, they must first get you or your computer to do something maliciously, like execute a code. The main offenders in malware realm are outlined below:

Malicious scripts

Most WebPages contained JavaScript with malicious code making the browser vulnerable and thereby granting admin rights to the users provided the browser lacks proper anti-malware software installed. Therefore, for you to be on a safer side, without you permitting attackers to compromise your machine, you need to first install anti-malware software to prevent an attacker infiltrating into your machine. Modern internet does not require a specific scripting engine that downloads and runs the code. The user needs just to visit a page. You execute JavaScript nearly every time you visit a website.

Infected files

Most internet users in Sierra Leone and elsewhere sometimes download malicious links containing malware that infect their files; such links or sites include screensavers and media codecs to name a few that hackers post containing malicious code. When internet

user downloads and runs them, they immediately become prone to attack and they are referred to as a “potential victim”.

Embedded media

Webmasters always insert media archives that online users normally click, and in turn, infect the whole webpage and make it vulnerable to attacks. Media players just like an OS regularly require an update. Unfortunately without proper patch implementation, it would be almost not feasible for users to keep their systems up-to-date.

Attack vectors

A dynamic website exhibits both pros and cons for internet users. Dynamic content is a process where everyone wishes to benefit from the revenue generated by an advertisement. This normally happens with the help of ads in the form of videos and audios prompting the users to click on them.

Owned websites

Some websites are usually owned by malicious online fraudsters designed to lure people into trusting such websites or hack into genuine websites to cause mayhem. They either motivate users to visit their fate websites or are already hacking into those websites via their homepage, favorites, and bookmarks.

Spoofed domains

It usually occurs as a result of either compromising a DNS or due to typographical errors deployed to exploit online users. Just typing a wrong letter turns a website into a hostile ecosystem. Failing to recognize such mistakes will expose your systems’ vulnerabilities which hackers will capitalize on and hack into your systems.

Phishing attacks

Phishing attacks occur when malicious attackers insert malware into someone’s machine with the help of the internet. Luckily, it can be easily being stopped if users would carefully pay attention. Phishing attacks are frequent with the fact that they are most successful. Sometimes clicking on a malware especially when you want to download a file or software on the internet, it redirects you to another webpage before downloading. It almost always occurs daily.

Cross-site scripting

Cross-site scripting attack allows online fraudsters to insert client-side scripts into weak web pages upon clicking grants their browser to execute the scripts. Hackers deployed them to snip personal data or download and install malware.

Malicious links

The majority of the internet users normally click on malicious hyperlinks in their emails, WebPages or a forum post. Attackers sometimes insert the malicious link into a discussion thread and wait for a possible victim to click on it. It may sometimes be attack-free or execute malicious code into a webpage.

Network sniffer

A network sniffer is a tool used to detect network problems thereby allows an individual to capture and view the packet level data on the network. According to the International Space Station (ISS), it is a tool that exploits the network interface of a computer to intersect data packets meant for other computers. It is also known as network monitors and analyzers and also collects packet-level data and information.

Network Sniffer Applications

Normally, network sniffer is there to analyze network traffic and bandwidth utilization, so that underlying troubles in the network can be identified. However, there are two usages of network sniffer:

Pros

The advantage of using network sniffers is to ensure that the network is properly maintained and works properly. The following are some of the merits it exhibits:

- Capturing packets.
- Recording and analyzing traffic.
- Decrypting packets and displaying in clear text.
- Converting data to a readable format.
- To reveal information such as IP, protocol, host or server name, domain name, and others.

There are several varieties of packet sniffing software with varied functions; some process hundreds of protocols, and others can only process one or two. TCP/IP, IPX, DECNet-ordinarily are the common protocols analyzed by a sniffer. It can deploy network engineers to monitor and analyze a network, detect a breach, control traffic or manage network activity. It can be used by intruders to break into computing systems as a snooping attack.

Cons

Wrong use of a sniffer normally harms network security infrastructure. The following demerits of network sniffers are:

- Hacking of passwords is the major intention for almost malicious users of the sniffing tool.
- Stealing of transactional records including password, username, account, credit ID and other relevant details.
- Listening and recording video messages or emails and replay them later.
- Manipulate computing details to cause damage.
- Destabilize the integrity of a network security features or access higher-level authority priority.

Sniffing is today the most vital tools in the defense of cyber-attacks and cybercrime industries due to advanced technology.

Conclusion

The world today is a hostile cyber environment where individuals or entities and/or individual nations conduct espionage activities either to gain competitive advantage or for financial gain. Most nations in Africa including Ghana, Kenya, Uganda, South Africa, Nigeria, and the developed ones have applied tougher policies to fight cybercrimes. We need as a nation to move at a faster pace to provide a safe and secure cyber ecosystem that will fascinate prospective investors into the country.

Furthermore, if strong cyber laws are legislated, it will help boost the economy and alleviate poverty, and also improve on the lives of average Sierra Leoneans. Also, the government should embark on the massive sensitization of the use of the internet, and how to protect their personal and government sensitive information from cybercriminals.

Chapter 4
Threats and Challenges

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

***Corresponding author:** Ibrahim Abdulai Sawaneh, Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

Introduction

With more groundbreaking discoveries, technology makes it very hard to safeguard online activities from cybercriminals. Cybercrime today is a threat to informationalization and digitalization that is causing digital instability disrupting global financial transactions in billions of U.S dollars [70]. The cyber threat is among the top four national security risks in the U.K higher than that of a nuclear attack.

Nations are a constraint on how to increase citizen's awareness of businesses operating in cyberspace. Organizations normally pay little attention to cybersecurity issues either for the high cost involved in regularly training staff or upgrading of existing security software and computing devices.

According to Lloyd's bank, the yearly mean cost to a company is currently $400 billion worldwide [71]. The estimated bill to an individual company is over $2.1 million on average [72].

Awareness Issues

Several challenging issues surround boosting cyber threats, and are outlined below:

Firstly, there exists a gap in communication between both private and public entities. The majority of critical infrastructure is privately owned. Most times, they are not willing to disclose security issues, which could certainly give a financial competitive advantage if

disclosed to rivalry institutions. As a result, information about cyber threats, challenges, and possible effects are not shared freely.

Secondly, the lack of cyber awareness among institutions with regards to critical infrastructures, particularly the incorporation of web-based interfaces into key monitoring gadgets that can be accessed anywhere. Devices are linked using the internet for several reasons, particularly infrastructures that can be accessed over larger geographical areas. It facilitates remote connection and control whilst saving cost. This allows engineers to monitor and work remotely without having physical contact in solving problems. They just have to monitor the systems from a point that houses the control system. However, some administrators manning such critical infrastructure pay less attention to the security of devices connected to a remote system.

Thirdly, lack of trust in the existing security schemes will indicate the awareness problem of the level of the preventive procedures with their effectiveness. An in-depth defense security mechanism is required to protect critical infrastructures. Each layer of the infrastructure has different security features that bared intruders automatically gain access to the next layer, as critical infrastructure possesses a harder outer shell with a softer internal system with regards to security. However, all the layers of security are either provided with multiple Intrusion Detection Systems (IDS) or Unified Threat Management Systems (UTM) facility that has vulnerabilities exploited through zero-day attacks.

Fourthly, spear-phishing cyber-attacks are done on a community level that deployed to reveal account details including passwords, users ID and name. The phishing attack is on the rise and the most common one is a spear-phishing attack where a victim is targeted through a phishing attack [73], with a success rate higher compared to the generic bulk method normally used. Spear-phishing attack is intended to target a specific victim in mind through exploiting human error and lack of threat awareness. The motive is to the fake potential victim with the assurance that an email-based scam is legitimate, guaranteeing that the data contained in it is specific to that person or organization [74].

Several private and public entities have been hacked using the spear-phishing attack as a result of poor understanding about the nature of the attack, and disclose sensitive information to third parties.

Cyber Attacks in Modern days

Cyber-attack is a hot topic in the modern-day as a result of groundbreaking findings in technologies and sciences as stated below:

Denial of service (DoS)

DoS attack occurs when a cybercriminal attempts to make a machine or network inaccessible to its legitimate operators by temporarily or indefinitely disrupting services of a host linked to the internet. DoS attacks are normally done by “flooding” the resource with a large number of requests [75]. This limits the server to reply to some or all authorized requests. Legitimate users who want to utilize the pool of resources are denied access to those resources. A single DoS attack is easy to manage, and a distributed denial-of-service attack (DDoS attack) originating from several sources. DDoS attacks involve several computer users willingly joining hands together to take an active part in the attack. The DDoS attack is generally orchestrated using botnets - networks of breached computers whose users are unaware that their machines are partaking in an attack [76].

Malicious online users normally attach high profile web servers, sites or services - online payment methods with credit card facilities, banking facilities, revenue collection departments, or blackmailing [77 - 79] with malicious software installed on computers that grant a third-party total control of the system.

Website defacement attack

A website defacement attack is a technique that manipulates website content without prior knowledge of the web administrator. This happens when an attacker disrupts a particular website, modifies its contents to deceive people who visit the site. It is electronic vandalism to motivates cyber protesters or hacktivists [80]. Several religious and government websites are breached by political or religious-inspired cybercriminals to spread political or religious beliefs to deface the views and beliefs of others.

SQL injection technique occurred in website defacement intrusion. The invader inserts malicious data in a web form [81]. Traditionally, SQL injection is easy to protect, as a result of a programming error on the website. However, in practice, several websites are exposed due to negligent security practices.

In contrast, in ÐDoS attacks, website defacement refers to a situation in which an intruder gains access to a target computing system. However, gaining access to an organization's web server is different from breaking into that organization's internal network, because web servers are normally hosted on a different network.

Other break-ins

Break-ins are a process where an attacker breaks into a system than a web server or break into web servers that store data than a public website. Such break-ins happen using methods analogous to those applied in website defacement. It depends on the level of IT security on the intended computer. Once an intruder is granted access to a computing system, they will be granted access to other computers within the same network stealing sensitive data and install malicious apps that turn the machines into zombies for a botnet or cause other destructions.

Cyber attackers

Several governments are faced with numerous challenges with regards to Cybersecurity. Findings indicate a surge in hacks and breaches of data globally. Studies further indicate that most organizations' data are not protected as a result of poor cybersecurity practices, and make them vulnerable to data loss [82].

Cybercrime

Cybercrime is a big threat to global businesses and governments. Cybercrime costs in 2017 increased with an organization's spending growing approximately 23% than in 2016 - on average roughly $11.7 million U.S dollars[83]. The average cost of malicious intrusion on an organization was around $2.4 million U.S dollars[84]. There was about a 22.7 percent increase in cybersecurity costs worldwide from 2016 to 2017[85]. The most luxurious element of a cyber-attack is information loss, representing about 43 %in costs[86]. Ransomware attacks costs surpass $5 billion U.S dollars in 2017, 15 times compared to 2015[87]. Loss related to cybercrime is expected to hit $6 trillion U.S dollars yearly by 2021[88].

Hacktivism

Hacktivism originates from two terms "hacking" and "activism". They are cybercriminals who penetrate hacking activities to penetrate computing systems or networks illegally for either social or political gain.

The rise of hate speech or radicalism through digital and social platforms across the globe has negative consequences: the Arab Spring of the Middle East, the green revolution in France (2019), several mass shootings (Texas and Ohio, 2019) in the U.S, the in the Sri Lanka bombing in April 2019, the Christchurch mosque massacre in New Zealand are

perpetrated using live stream using social networking sites (Periscope, Facebook, Twitter) with online users participating in the online debate. Mayor Ada Colau of Barcelona amassed massive online support approximately 6,000 people for his electoral campaign in the public assemblies, with the establishment of the network of cyber activists [89].

They attack influential and powerful people's computer networks anonymously and sometimes terrorize organizations. The Panama Papers exposures by Wiki Leaks and Edward Snowden are referred to as "Hacktivism". Her documents are amassed, leaked and spread through the internet with political ramifications. The Panama leaks orchestrated massive protests making the Iceland Prime Minister quit office and calls for similar action in the U.K [90].

Cyber espionage

Espionage is an effort made by either an individual or state to extract sensitive information from a rivalry state or individual organization [91]. Cyber espionage is acceptable behavior as compared to cyber-attack, which is unacceptable behavior following international law.

Several objections have been among the world powers against unacceptable cyber espionage prompting fear of a new era of informationalization and digitalization war. Furthermore, the U.S has been advocating for new standards for cyber espionage, permitting nations to practice it only for traditional intelligence purposes to make critical national security actions. Cyber espionage is becoming a normal order of the day among the world powers. An ex-CIA agent pleaded guilty spying for China, according to the U.S justice department in May 2019, as the main reason believed for dismantling the U.S espionage network.

Prosecutors indicated that Jerry Chun Shing Lee was financially motivated to disclose information on the U.S covert assets. About 20 informants were murdered or jailed between 2010 and 2012 becoming most catastrophes in the U.S intelligence in modern time [92].

Conclusion

Cyber-attacks are on the rise in the global cyber helm as a result of individual or state-sponsored activities. It mainly perpetuated to gain either financial rewards or gain an edge over an individual, company, businesses or state. Some used it to blackmail their victims and others for espionage purposes.

The cyber unit of the Sierra Leone Police Force intercepted and apprehended some Chinese and Ghanaian fraudsters stationed in Sierra Leone in 2019who were involved in massive Smartphone cyber-attacks costing millions of U.S dollars. Their scheme operated on a global scale. The cybercriminals were handed over to the CID for criminal investigation, though they claimed their company was legitimately licensed and registered to operate in Sierra Leone.

Global System for Mobile Communication (GSM) operators were mandated by NATCOM to register all their subscribers within the country. The move was expected to help the various security agencies and network operators to easily identify Smartphone fraudsters. Furthermore, the Ministry of Technical and Higher Education and the Tertiary Education Commission (TEC) should develop curricula in cybersecurity studies to be taught at various levels to increase the awareness in cybersecurity in the country.

Chapter 5
Digital Risk Assessment in the 21st Century

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

***Corresponding author:** Ibrahim Abdulai Sawaneh, Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

Introduction

As informationalization, digitization, bid data extraction, and IoT continue to grow rapidly in the 21st century, with more innovative ideas and schemes unearthed, the threat to personal information becomes a dilemma for individual states and companies to tackle such cybersecurity threats. Therefore, security agencies and governments around the world should be vigilant in solving or minimizing cybersecurity threats by unanimously adopting robust security measures that tackle such threats either internally or externally.

Digital Risk

The world is gradually becoming digitalized, which is constantly changing the world we lived in today. Both public and private entities have gone digital, because of the informationalization and big data technologies that are compelling digitization. The workflow and infrastructure of public and private organizations are changing to a more well-organized and manageable process. Informationatization and data analysis with the aid of computers perform complex tasks digitally in a few seconds as compared to analog or manual operations. For instance, a supercomputer deployed at Heathrow International Airport in the U.K can process millions of airport data digitally within a minute, provides passengers with comfortability and protection to their data.

The Role of Cyber Security in Minimizing Online Crime Rate in Postwar Sierra Leone: Office of the National Security (ONS), and the Cybercrime Unit at the Criminal Investigation Department (CID)

Furthermore, complex processes can be controlled and monitored from long distances, employees have access to networks and databases, and automation is making manufacturing more efficient and effective. With all the pros attached to digitalization, yet it still has few cons, it falls into the hands of cybercriminals. With the advent of IoT, where almost all electronics and communication devices are interconnected to the internet poses a digital vulnerability, where cyber-attack are the current security threats in the digital age. Society relies upon the undisturbed functions of infrastructures and their services. A failure in one of these infrastructures or services may lead to serious consequences, such as loss of life, financial damage, environmental damage, or compromised functions of authorities. Digital systems are exposed to risk from organizational decisions, and technical and human failure. Unwanted events can also be caused by actors with harmful intent through cyber-attacks. Cyber-attacks lead to loss of secretive data or manipulating data and information, or causing accidents and sabotage by taking control of production systems. The increased connectivity comes with a risk, a cyber-risk.

What is Risk?

Risk is viewed as an undertaking within a specified timeframe leading to some future consequences [93]. According to Aven, these consequences are unknown, uncertain and include both positive and negative outcomes. The outcome of the consequences may either be undesirable or desirable. A risk description is defined from the event, assumed consequences, a description of uncertainty, and background knowledge or information [93]. Table 5.1 and Table 5.2 adapted from Aven (2015, page 15) to describe digital risk:

Digital Risk
Consequence: The occurrence of a cyber-attack of a specific type (known or unknown types) and its time occurrence, and its consequences for an organization (loss of data, production interruption, etc.).
Uncertainty: Today we do not know if the organization will be exposed to one or more of these cyber-attacks, and we do not know what the consequences will be.

Table 5.1: Digital risk.

Digital Risk description
Event: The organization is exposed to a specific type of cyber-attack next year.
Consequence: The organization's consequences are simplified in four categories: 1) the organization suffers production stoppage, 2) reduced production speed, 3) loss of important data, 4) no consequences.
Uncertainty: Based on the information acquired via our process, we can express the prospect of such an event and the consequences. This can be a quantitative or a qualitative expression of the uncertainty.
Knowledge: the knowledge we have based on the assessments are data, information, models, justified beliefs and assumptions.

Table 5.2: Digital risk description.

Uncertainty

Informationatization and massive data transfer especially the newly launched 5G technologies are accompanied by uncertainty, which means, it can be biased, wrong, or partly true. Like most decisions and assessments, they are done without a 100% certainty and complete access to information. In situations where there is high risk and large uncertainties, it is difficult to predict the consequences or outcome of the

decision. This affects the quality of the risk assessment. Sometimes, the risk assessment process contributes more value than the actual probability that an event occurs. The risk assessment is a tool in which the participants get acquainted with the possible events and their consequences. The assessment guides the management or risk assessors through a process that proves an outcome (or probability) given a set of information, models, or data that carries uncertainty. The process can strengthen risk awareness and at the same time, demonstrate to the management what the results are based on. If not properly managed, a risk assessment can give a false understanding of risk by narrowing it down to a specific number without explaining the reasoning of the conclusion.

In the matter of digital risk, there is the emerging threat of sabotage, espionage, and cybercrime from criminals, hackers, and nations. This risk picture is evolving and the probability of any form of cyber-attack changes with the increasing number of malicious actors and their access to sophisticated tools and methods. As organizations depend more on digital systems to function, the organizations are more vulnerable and can suffer large consequences if not properly secured. This implies that a risk assessment should be done regularly with updated background knowledge, as the risk picture is constantly evolving. Digital risk is developing and black swans can emerge due to low-risk awareness or a smart cyber-attack which utilizes an unknown exploit. A black swan is a surprising, extreme event relative to present perception and knowledge [94]. These events may have catastrophic consequences for the organization, environment, and humans. There are three types of black swans [95]:

- **Unknown unknowns** - Events that are completely unknown to the scientific environment.

Unknown viruses and methods can occur as the criminal actors become more cunning and sophisticated in their methods. In some incidents, the attackers use a zero-day attack, such as Stuxnet, which means that there has been no record of a similar event from the time the threat becomes active. These events rely on highly competent personnel and resources to be able to respond and reduce the consequences of such an unknown threat.

- **Unknown knowns** - Events that are not on the list of known events from the perspective of those who carry out risk analysis, but known to others. Unknown to some, known to others.

The competence level and resources within the organization depict how the information of digital risk is utilized, which makes some organizations more aware of risks than others. The prioritizing of digital risk and risk assessment, in general, makes a difference to how well the organization knows about black swans.

- **Knowns** - But not believed to occur because of low judged probability.

Each organization has access to and can allocate resources differently. Some organization's benefit of preventing some unlikely scenarios is best not to be bothered with. This prioritizing may have something to do with the size and the values created by the organization, and how much of digital technology they use.

Risk acceptance criteria (risk tolerability limits) is the organization's predetermined limit to how much risk is acceptable at a given time. If the calculated risk is within the range of this value, then it is acceptable. Otherwise, the risk is unacceptable (intolerable), and risk-reducing measures are required [93]. It should be calculated to fit the organization's ability to carry risk. All risks should be reduced by following the ALARP principle (as Low as Reasonably Practicable). This principle means that the benefits of a risk-reducing measure should be assessed with the disadvantages or costs of the measure [93]. This implies that a measure should be implemented if it does not create a significant disadvantage for

the organization, such as high costs. This suggests that there will be differences in risk acceptance criteria and the ALARP principle of industry companies. For example, in a large organization, such as a highly profitable international oil and gas company with 30,000 employees, and a smaller organization, such as a steel structure production company with 15 employees. These two organizations will have different risk carrying capabilities.

Cyber Security Risk

A cybersecurity risk classifies the various information assets that could be exposed to a cyber-attack and categorizes the various risks that could negatively affect those assets [96].

Cyber Security Risk Assessment

Risk Assessment is a process of identifying, analyzing and evaluating risk. It allows the organization to choose the best cybersecurity features that affect their organization. Without a risk assessment scheme to carefully select the appropriate cybersecurity options, time, effort and resources will be wasted - notwithstanding, there is not enough time to implement measures that defend against actions that are unlikely to happen or won't have much measurable impact on the organizations [96].

Moreover, you may likely undervalue or overlook the risks that will cause substantial damage to the organizations. This is why so many best-practice, frameworks, standards, and laws - including the GDPR (General Data Protection Regulation) and DPA (Data Protection Act) 2018 require them [96].

Cyber security risk assessment components

A cybersecurity risk assessment examines numerous information resources that will be exposed to cyber-attacks including hardware infrastructure, confidential data, critical infrastructure, networks, and software, by identifying the numerous risks that could disrupt those assets. A risk assessment is normally done as a way to select the appropriate controls that solve the identified risks. It is vital to constantly monitor and review the security risk ecosystem to identify changes based on the organizations 'perspective, and to sustain an overview of the comprehensive risk management processes.

ISO 27001 and Cyber risk

The International Standard ISO/IEC 27001:2013 (ISO 27001) offers the best practice specifications known as ISMS (information security management system) - a risk-based assessment that manages people, processes and technical security features. Clause 6.1.2 set out the standard requirements for an information security risk assessment scheme indicating that organizations should:

- Establish and maintain certain information security risk criteria.
- Ensure that repeated risk assessments "produce is consistent, valid and comparable results".
- Identify "risks associated with the loss of confidentiality, integrity, and availability for information within the scope of the information security management system", and identify the owners of those risks.
- Analyze and evaluate information security risks, according to the criteria established earlier.

It is vital for organizations to "Retain on the information security risk assessment process", which will prove compliance to those risk requirements. Other processes are also followed in creating the relevant documentation, as part of the information security risk management procedure.

It Governance Risk Assessment Services

Assessing the cybersecurity risk assessment process is a serious task as effective planning is required with professional knowledge including all people-, process- and technology-based risks. Without proper guidance, it will only work on a trial and error basis. IT Governance addresses a range of risk assessment and cybersecurity services that suit all security requirements.

Cyber Health Check

The cyber health check is a consultancy and audit based practice that assesses security vulnerabilities remotely and also performs an online survey to evaluate cyber risk threats to find a practical means to mitigate the risks. The aim is to detect cyber risks, audit the responsiveness of the threats, analyze the real risk threats and then create a prioritized action plan for handling those threats following the organizations' objectives.

vsRisk cloud risk assessment tool

vsRisk Cloud, an online risk assessment utility use to solve tougher security risk assessment expensive in nature that saves time and effort. Allied with ISO 27001, it continuously updates the risk assessment procedure in delivering reliable cybersecurity risk assessments.

Why choose IT governance

IT Governance tackles risk management and provides effective solutions with regards to cyber resilience, data protection, GDPR, Payment Card Industry Data Security Standard (PCI DSS), ISO 27001 and cybersecurity. It falls under the following frameworks:

- U.K government CCS-approved supplier of G Cloud 9 services.
- CREST certified with ethical security testers.
- Certified under Cyber Essentials Plus, the U.K government-backed cybersecurity certification scheme.
- Certified to ISO 27001:2013, the world top recognized cybersecurity standard.

Threat

Generally refers to objects and people posing a possible danger to assets through attacks.

Threat agent

It is a particular object or person posing a danger by performing a cyber-attack. The DDoS attack is an example of a threat provided, if a hacker carries out a DDoS attack, s/he is called a threat agent.

Types of threat agents

Threat agent differs based on the intentions for carrying out such acts. The most notable ones are those actively engaged for monetary benefits, and some are motivated by political, ideological, religious, and national security reasons. The primary motive depends on what the attackers want to realize in an attack [97] as suggested in Marinos, Belmonte, and Rekleitis "eight different threat agents".

Cybercriminals

The cybercriminals exploit advanced tools and software illegally to gain from their malicious actions [98,97]. Usually, the cybercriminals belonged to a well-organized group having access to huge data resources as a result of their technicality and experiences. The inspiration lies in monetization and "show-of-skill".

They are usually involved in massive cyber frauds with an in-depth attack analysis. The techniques are made possible due to the innovations in technologies and businesses, including e-finance, e-commerce, e-payment, and bitcoins. They viewed it as "as-a-service" and can potentially be involved in espionage-as-a-service [98,97]. They also create malicious tools to deceive their targets through the internet. The anonymization, encryption and virtual currencies make it hard to identify and considerably hinders the detection process.

Insiders

Insiders are people working within institutions including; staff, suppliers, contractors, consultants, end-users, cashiers, executives, business partners and clients [97]. The motive of such acts is essentially based on monetization, betrayers, marginalization of aggrieved employees, or the convenience of bypassing the existing preventive security processes. Rivalry competitors usually recruit insiders for their agenda. It is less likely that a system admin misuses its system rights [97].

Online social hackers

They are actively involved in activities that produce other cyber threats [98]. They are generally categorized as highly experienced and talented attackers who monitor the behavior and psychology of their targets. Such social hacking tools include analyzing information, profiling users' loggers, social site accounts, or breached data. The prominence and occurrence of phishing attacks have to improve and allow further abuse[97]. The group is usually involved in identity theft and stealing of confidential personal data and user credentials.

Cyber spies

Cyber-spies are on the rampage with huge material and financial assets that comes either from government or corporation [98]. They are a well sophisticated, resourceful and innovative groups, with highly sophisticated tools design to hack into cyber-physical systems [97]. Governments around the world have designed cyber intelligence schemes that are inspired to gain intelligence concerning sensitive information such as; state critical data, military top-secrets, healthcare records, trade secrets, and acute infrastructure, and other essential records. The global communities should enact stronger international cyber-espionage policies and judicial rules limiting such practices. With the non-existence of such policies, rivalry and powerful nations have been accusing each other of cyber espionage that has resulted in confrontation among powerful nations, such as China and the U.S, U.S and Russian, North Korea and the world, Russian and the E.U, and other occurrences.

There is an increase in corporate-sponsored cyber-espionage targeting other corporation's records [98]. Generally, they are involved in malicious activities such as data breach and data intrusion. The inspiration is to gain competitive advantage, counterintelligence, stealing sensitive business information, and abuse intellectual property rights, saboteur or influence competitors [98].

Hacktivists

They depend on media coverage for their actions [98], such as, DDoS attacks, leakages and publishing information. The group is driven by political motives, social injustice, and gears towards influencing political decisions. They are dynamic meaning that they do not necessarily have a centralized organizational culture. They may comprise of several threat agents with a common cause, but different motives. They normally surface during political tensions and injustice towards particular social groups. They surface during riots, global sports activities, and other key events with global attention [98]. Some hacktivists in

2015 did focus on the assumed wrongdoings, promotion of freedom of expression, and an open internet [97]. For instance, the Arab Spring, which includes the anti-government protests and armed rebellions that swept across North Africa and the Middle East in 2010. It was attributed to repressive governments and poor standard of living, beginning with protests in Tunisia [99-100]. Similar unrest provokes protesters in Sudan, Algeria, Venezuela, and Zimbabwe in 2019.

Cyber fighters

Cyber fighters are citizens who have momentous remarkable power [98] and include cyber terrorism, hacktivism, and cyber espionage. They are driven by politics engaging in saboteur activities when their political, national, or religious values are threatened. It is mainly designed to cause mayhem that attracts media attention. Traditionally, they act on the orders of totalitarian governments [98]. Nowadays, they are becoming more sophisticated with the advance in technological innovations on the market.

Cyber terrorism

They mainly attack nations, communities, and critical infrastructure, and engage in large-scale sabotage to cause harm and promote violence [98]. Their drive is motivated by manipulating political decisions and actions based on their political motives or dealings. They utilize advance tools to avoid state surveillance while communicating, recruit new members globally, collect, and distribute anonymous financial transactions [98, 97]. They are endowed with advanced communication knowledge and malicious tools with varieties of attack schemes using cyber-crime-as-a-service.

Script kiddies

They are normal teenagers who are motivated by hacking through the use of malicious tools [98]. They viewed it as a sign of possessing high skills, achievements, and hacking as a fun game. Several materials and tutorials are available on the internet on how to perform cyber-attacks with the aid of malicious software. They are not highly skilled hackers and lack the proper knowledge and consequences and self-control to carry out large-scale cyber-attacks [98].

Non-Malicious Situations

Digital and electronic infrastructures are vulnerable to human, organizational, and technological errors. Natural catastrophes including fires, floods, hurricanes, and earthquakes can lead to a possible failure in those infrastructures, and trigger risk in digital and electronic systems caused by management decisions, technical and human errors.

Vector

It describes how the hack is carried out and includes the following:

Typical Attack Vector

There are many ways of exploiting weaknesses in a system. The most successful exploits demand careful planning and research, as well as access to tools and software that can perform the preferred task. **Figure 5.1** shows a typical representation of a multi-stage attack.

Lloyd's in 2010 stated that the attackers may play a long game, with repeated attempts to complete their objectives. This means that the extraction of data can take many months, obtaining a little bit of information each time until the attacker can piece together enough to establish a foothold into the system. The attacks usually accomplish the objectives

via a mix of social engineering and malware. Particular individuals and information are targeted, and the attackers are careful to cover their tracks. Once a foothold is secured, the attacker spreads into other systems. The most sophisticated attack, often known as an advanced persistent threat (APT).

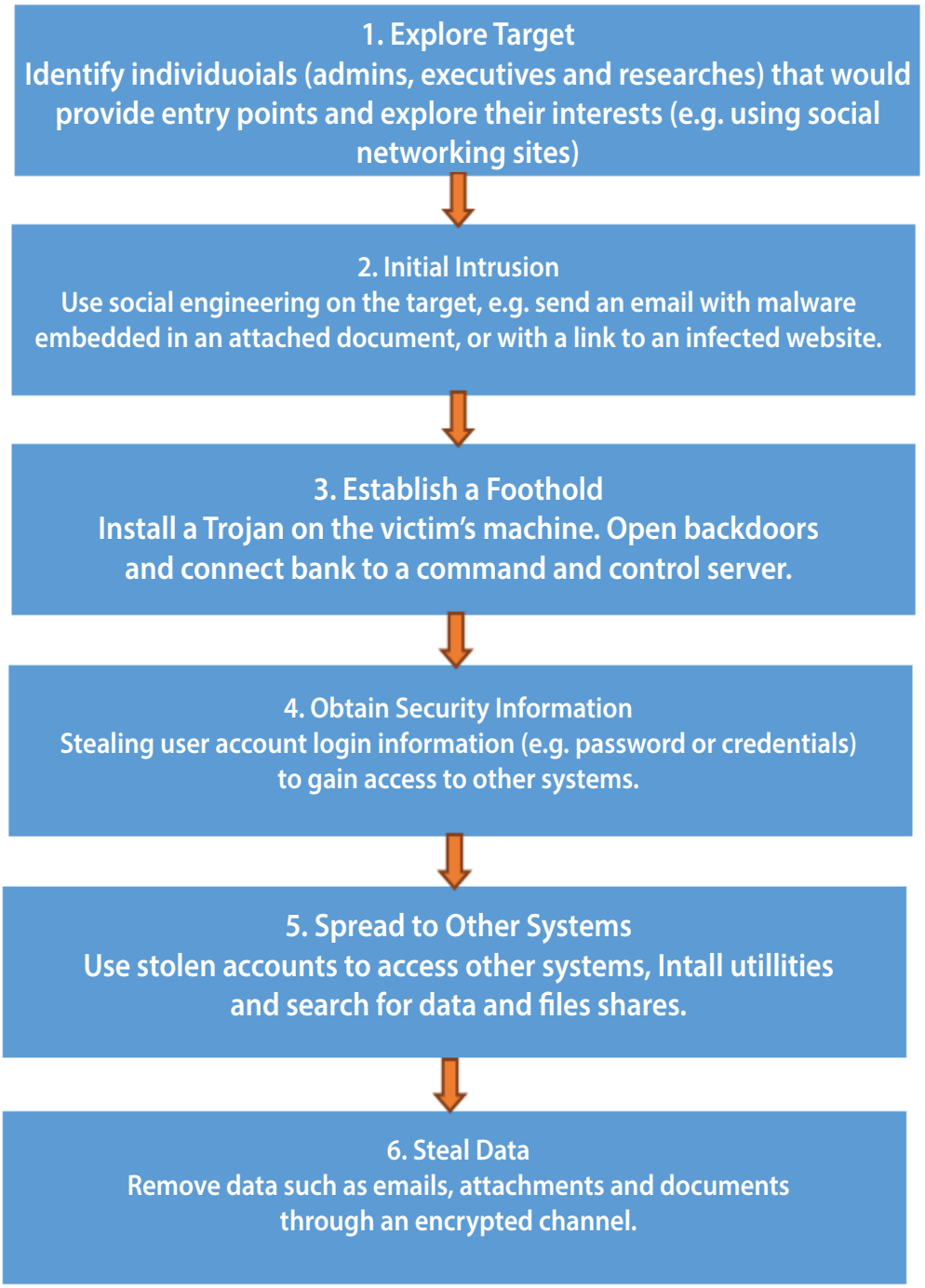


Figure 5.1: Multi-Stage Attack Representation [**101**].

Discussions

War Against Cybercrime

In combating mobile crime and mobile-money laundering frauds, NATCOM and all Mobile Network Operators (MNOs) conducted a massive sim cards registration and verification nationwide. The sim card registration and verification exercise were done to safeguard Mobile Network Operators strictly adhere to their responsibilities as enshrined by the "SIM Card Registration Regulation of 2009". It also guarantees the provision of secured telecommunications and mobile financial services, and possibly eliminate the proliferation of online frauds, and safeguard national security [102].

In a news conference held at the commission's headquarters in 2019, all the MNOs including Orange, Africell, Sierratel, and Q-Cell vowed to address mobile frauds by registering all their subscribers countrywide. Mr. Sahr Sowah, director of regulatory administration at NATCOM indicated that cybercrimes via mobile networks have increased in 2019, which prompt NATCOM to mandates all MNOs to undertake the sim card registration and verification exercise. "We are giving support to MNOs and also send a clear message to their customers that it is mandatory to register all sim cards," he said.

WAEC fraudsters

Public examination faces a huge task, as students are engaged in cheating with the help of mobile phones that have got an internet facility. The accomplice answers the examination questions and sends them via WhatsApp to students in the examination halls, which is against the "New Direction Government Education Policy". It demands students to study pay greater attention to their education. "Paying people to write the examination for you and also involving yourself in examination malpractices only put you into trouble", AIG Brima Jah of the cautioned parents and students. He calls on the parents to support the "government quality education policy" to encourage their children to study very well and avoid partaking in examination malpractice [103].

Therefore, the researcher recommends that government institutions with the mandate deliver quality education not allow students to enter with their mobile phones into the examination hall.

Financial intelligence unit

The introduction of "Mobile Money" transfer by the two dominant mobile networks Orange and Africell raised some issues, such as security, corruption, and money laundering. The majority of the banks in Sierra Leone embraced mobile banking to conduct transactions such as to deposit, collect, make online payment and transfer. Therefore, MNOs and security agencies should vigorously monitor online financial transactions to prevent money laundering and financial terrorism [104].

Conclusion

With groundbreaking innovations in modern times makes it hard to protect personal data and government information from potential intrusion from cybercriminals. Cybercrime is the order of the day and raises global concern; with mounting digital threats disordering the global economy with billions of U.S dollars [70]. In the U.K only, cyber threats classified among the top four risks to national security, which is more than a nuclear attack.

The key tasks for governments internationally are how to increase the awareness of citizens and businesses concerning prevailing cybersecurity threats. Several organizations ignore this aspect due to the high costs involved in implementing a security system or training of personnel in security measures.

Furthermore, cybersecurity studies should be introduced into the education curricula starting from elementary schools to universities and technical vocational institutions. Subsequently, it will create earlier awareness of security issues and further protect our information. The deployment of CCTV cameras in sensitive locations and offices will likely minimize cybercrimes in the country. To fight against online crimes need maximum collaboration among governments, security agencies, and the public. Creating awareness of the preventive methods will certainly reduce the numerous crimes about online platforms.

Chapter 6
Vulnerabilities and the Way Forward

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

*__Corresponding author:__ Ibrahim Abdulai Sawaneh, Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

Introduction

One of the greatest threats of today is how the government protects its doorsteps against cybercrimes with the advent of informationalization and digitalization. The threat is growing towards digital and information systems, and therefore, developing nations need to streamline their security platforms with digital technology and digital infrastructures. Because of massive corrupt practices by most African governments, they pay less attention to how they should protect their nations from cybersecurity threats and challenges. Developing nations should strategize countermeasures to combat the growing cybersecurity threats and challenges facing their cyberspace. Therefore this chapter will discuss some of the vulnerabilities also those that have been discussed in chapter 5.

Vulnerability Management

Vulnerability is a weakness in a system that makes it likely an undesirable event happens, or a desired one fails to happen, and it affects greatly data security [105]. Cyber vulnerabilities are vulnerabilities that include those weaknesses or errors associated with system hardware and software used in an organization. Here, only three types of vulnerabilities will be discussed: human vulnerabilities, organizational vulnerabilities, and technological vulnerabilities.

Human vulnerabilities

Human vulnerabilities are characteristics and behaviors that create, exploit, or contribute to the misuse of a system weakness [106]. It could either be unintentional behavior including errors that lead to such vulnerabilities or enable their misuse, as well as deliberate malicious activities such as exploiting the vulnerability. Note that every employee within an institution can become an attacker. A security breach which occurred as a result of unintentional behavior cannot only be blamed on individuals, but also as a result of the errors in the design of such systems and how the employees are managed. Human vulnerabilities or weaknesses should be carefully diagnosed and managed before a security breach occurs. Currently, a tendency to overlook undesirable features and behaviors until such a security breach occurs exists, but un-acknowledging such vulnerabilities can lead to systemic failures. It would be wrong basically to compare human vulnerabilities to "undesirable behaviors." Such characteristics or behavior leading to a security breach in a specific situation may be extremely desirable in another, such as being helpful to end-users, or having complete trust in colleagues). Here, five keys issues are discussed below:

Competence

Most public and private institutions in Sierra Leone lack technical know-how and competence in the field of cybersecurity and information security. Some even lack the basic ICT skills on how to protect their online data. This is because cybersecurity is a new phenomenon in Sierra Leone. Cyber competence is a prerequisite for good user behavior. It shows how ones respond to security threats; manage both internal and external media devices. No system is 100% secure, but at least requires some level of expertise to manage it. Fortunately, the "New Direction Government" placed a high value on science and technology. Scholarships and grants are assigned to science students in high schools and universities. The government of Sierra Leone also provides scholarships to deserving students to study abroad, all to boost ICT competence for the future of cybersecurity and its related disciplines.

Compliance

Sometimes, either public or private organizations normally fail to follow the routine security check, especially in developing countries. It emanated from a lack of knowledge in the field of information security, or maybe the cost assigned to such services by security experts. Some organization fails to divulge sensitive information to people who are not an integral part of the top management, with fair that it may be revealed to the outside world. This hinders compliance. Deviating from security checks will lead to the systems vulnerable to cybercriminals and hackers.

Awareness

The best way to manage security within an organization is through communication and cooperation among management, security experts, and employees. Senior management should constantly communicate security policies to employees and receive feedback which is then sent to the security experts to assess for security vulnerabilities within the system and subsequently address those issues. Therefore, for effective security practice, an organization should always make its employees aware of the security routines and ensure those routines are practice daily to avoid security risk.

Education

Today, almost every homes, offices and factory have at least a computing device to process information and make work lighter. The use of such devices requires some level of expertise, in which most people outside the security sector have little knowledge

and effects. Therefore, to follow the daily security routines, there should be a form of education. For instance, an organization such as the banking sector or immigration department should educate its employees on security issues regularly. This will help them to follow the security norms and make their systems more secure and safe.

Training

As technologies continue to grow, so do the people using them are require some form of education on how to use them. Training is necessary, as it alerts its users of the new updates and provides security parameters that render it more secure and addresses previous vulnerabilities within its systems.

Organizational Vulnerabilities

Organizational vulnerabilities are vulnerabilities that include the following:

Security Framework

The security framework is the basic procedure organization uses to counter cybersecurity threats. Organizations normally develop a framework for information security management and traditional HSE (health, safety, and environment). Having a poor security framework renders an organization vulnerable to threats within and outside the organization.

Risk management

The ability to perform value, threat, and vulnerability assessments are critical for gaining an overview of the organization's operation and system, threats, and the capability to evaluate the effectiveness of the security procedures and activities. The risk management and assessments should have a practical impact and should not be done out of compliance with regulations. The lack of a realistic risk assessment including the different disciplines of the organization is vulnerability.

Leadership engagement

Most organizational leaderships in developing countries lack basic ICT skills and engineering systems, thereby negatively affecting the security processes. The organization may get into unfortunate circumstances as a result of the lack of proper security procedures related to the use of third parties. Poor resource allocation to cybersecurity experts is sorely the responsibility of those decision-makers.

Collaboration

A division within an organization may lead to poor cooperation among the employees. This will cause employees to overlook basic security processes thereby exposing the system too a hostile environment making the system vulnerable. The organization is at risk of becoming outdated as it lacks external input from organizations that have different experiences and solutions.

Employee training

Employees with continuous training on security parameters will make an organization more secure and safe. It is the responsibility of an organization to continuously provide ICT behavioral knowledge, awareness and competence for its employees. Any organization that fails to create ICT competence and awareness may probably face unfortunate situations due to a lack of situational awareness, technological competence, and reporting routines.

Emergency response

Any organizations need to document ICT emergency response plan, teach its employees reporting patterns, document procedures, all to mitigate organizational security risk and save millions of dollars.

Supply chain management

As supply chains become fragmented, it is important to understand how organizations and systems are connected. Additionally, the use of third parties may challenge security assurance, control, and quality management. This means that the gap between the customer and service provider can reduce the customer's ownership of the operation/ system.

Technological Vulnerabilities

Technological vulnerabilities are vulnerabilities caused by technology and include:

Consequence Reduction

It refers to the ability to reduce ICT incidents and consequences in the workplace. This includes functions such as system recovery, redundancies, and the ability to operate with manual procedures.

Incident detection and response

A mechanism that allows the organization to detects incidences and appropriate response to those incidences following the incident detection response mechanism. It may contain guidelines and instructions on how to react when an incidence occurs, incidence response and emergence response mechanism.

User and access control

An organization must have the capability to monitors its user and access control system to detects any security flaw in the system caused by either its user's or system's failure. It may include a general overview of system users, their access and regular overview revisions to protect the organization from a possible cyber-attack.

System technology management

One of the main obligations of an organization is to protect its system software and hardware, and operations from malicious activities. Failure to follow the normal security routines will possibly be a catastrophe to the organization's stability. Employees must be able to possess some ICT skills that will monitor the security features of their systems.

Physical security

The organization must be able to establish physical barriers, security zones, and standard security protocols. Not all employees should be granted access to sensitive security zones in the organization. Proactive measures should be initiated to avert cyber-attacks against the organization's physical equipment.

Examining the Cultural Impacts on Cyber Security

Cybersecurity is gradually becoming the main concern for all nations around the world. Nations heavily depended on it to secure their information and critical infrastructure within the cyberspace. The U.S due to internet connectivity has the most commanding leads in cyber warfare and cyber espionage. It also makes them vulnerable, for instance, the alleged Russian melding into U.S 2016 elections.

Governments of developing nations should create strong cyberculture that will make security awareness a priority in safeguarding their nations against cyber-attacks. For instance in Sierra Leone, there is no cyberculture and in fact, most internet users and office workers either in the private or public sectors are not alert of the significance of not having cohesive cyberculture in place. Also, about 90% of the youths use the internet but lack the basic ICT skills to protect their online activities, especially when using the social media platform.

A questionnaire developed to investigate the loopholes in the security infrastructure in Sierra Leone indicated that safer cyberculture is needed to tackle the prevailing cybersecurity challenges. Sierra Leoneans, especially those in government departments, private businesses, individuals, telecommunications companies, ICT experts, schools, colleges, and universities should work as a team to fight against cybercrimes. To maintain and enhance secure cyber cultural practices in the country, education and training will be needed to create awareness on key security issues that lead to cyber-attacks. Civil servants and employees of private sectors should be given vital tips and awareness into the vulnerabilities if safer and secure security routines are not followed. For instance, people working in the defense department, banking industries and critical infrastructure should develop robust security measures into the consciousness of all employees.

A well develops schemes on the use of passwords on computing devices in government and private offices should be established and monitored. Employees must also be aware of social engineering impact. Humans relied on computers to virtually do everything from home chores to office functions. People are normally in the habit of connecting to free public Wi-Fi, not knowing the negative consequences as hackers may intercept and steal sensitive information, such as passwords, bank details, and others.

Conclusion

As technological innovations continue to break new grounds, so hackers are determined to break those systems. With the help of online software, manuals and tutorials available freely on the internet, more people are involved in the business of hacking. This means, governments, and organizations should mechanize robust security procedures and training for their employees. They should strictly follow normal security routines to countermeasure any security vulnerabilities. Continuous security awareness and training should be provided to all employees within the public and private sectors to avert possible cyber-attacks that will create vulnerabilities to the system. Also, sensitive information should be kept secret within the organization and only little senior management should be allowed to perceive such information. This ultimately will minimize insider attacks and makes the environment more secure. Finally, organizations should continuously update their software and hardware to match the present and future security challenges that will mitigate system vulnerabilities.

Chapter 7
Results and Findings

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

*__Corresponding author:__ Ibrahim Abdulai Sawaneh, Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

Introduction

The study examines the role of cybersecurity to minimize online crimes in post-war Sierra Leone. This chapter discusses the findings and impacts of internet crimes in third world countries. The researcher conducted thorough investigations into the causes and effects of the rising cybercrimes rate in Sierra Leone.

Data Analysis

The questionnaire of the study is a self-assessment mechanism designed to investigate the common root cause of cyber threats and challenges, which will help the state security apparatus to strengthen and enforce security measures in this antagonistic environment. Sierra Leone is a nation that has lately embraced technology to improve on the dilapidated security infrastructure after the bloody civil war in 2002. It has a weak cybersecurity infrastructure with a lesser number of cybersecurity experts in the state security sectors. By looking into areas such as effective management policy, the physical security domain, and logical security domain within the security framework in Sierra Leone, cybercrimes will be greatly mitigated making society a better place to live. About 100 questionnaires were distributed among selected security departments in the Sierra Leone Police Force, NATCOM, ONS, Ministry of Information and the private sector in Sierra Leone. About 65% of the respondents returned the questionnaires, which shows the researcher was able to examine those responses and make sound judgment based on the questionnaires received.

Security Apparatus	Top Management	Middle Management	Operational Management	Total
ONS	5	5	10	20
NATCOM	1	3	6	10
SLP	7	10	13	30
Ministry of Information and Communications	1	3	6	10
Private Sector	10	10	10	30
Total	24	31	45	100%

Table 7.1: No. of respondents by security apparatus.

Source: 2018-2019.

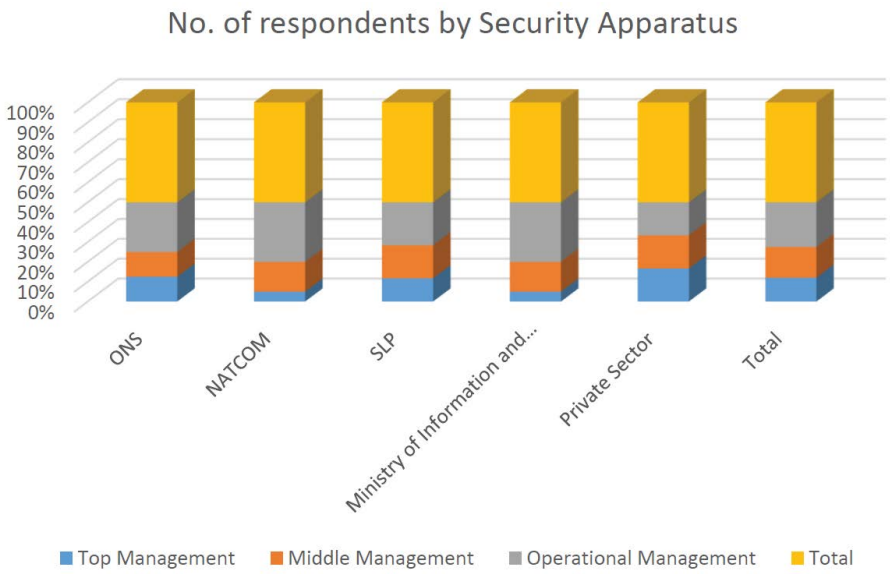


Figure 7.1: No. of respondents by security apparatus.

Source: 2018-2019.

Figure 7.1 shows that more than half of the respondents returned the filled questionnaires. Among the five security departments, SLP and the private sector top the chat followed by ONS, and NATCOM and ministry of information and communications were at the bottom of the chat. It was not easy in obtaining security information from the respondents, because of fair that the researcher will reveal them to the public. Therefore, the researcher was limited in detailing the full security details and was only able to analyze and give the tricks deployed by the cybercriminals, as a way to avert possible cyber-attacks.

Cyber Awareness Among The Five Categories Of Respondents

The majority of the respondents among the five categories chosen for this research have little knowledge about cyber-related activities, and only a few percentages believed to have cyber awareness. About 5% of the respondents believed that their knowledge with regards to cyber activities is extreme, 4% is thought of having very good awareness.

Response Level	Percentage (%)
Extremely	5
Very	4
Moderately	15
Slightly	6
Not at all	70
Total	100%

Table 7.2: Percentage of cyber awareness level.

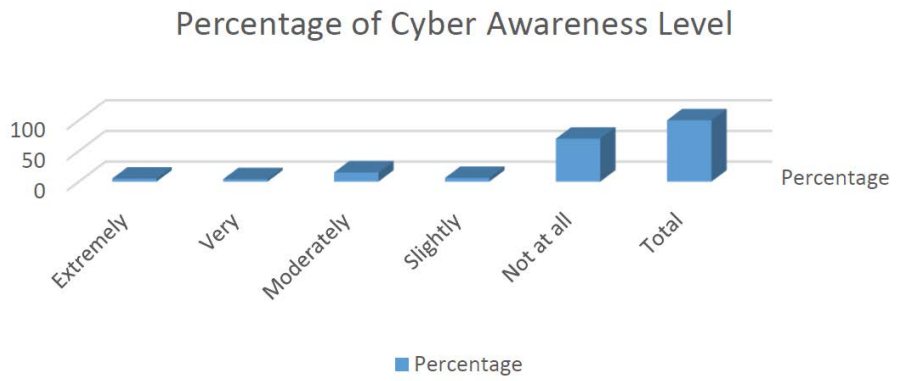


Figure 7.2: Percentage of cyber awareness level.

Source: Questionnaire, 2018.

15% of the respondents have moderate awareness with 6% having slight knowledge, and 70% of the respondents do not know about cyber-related activities. This shows that the majority of internet users in the country are vulnerable to cyber-attacks, due to the unawareness of the impact of cyber-related crimes.

Cyber education

Cyber education in Sierra Leone is necessary as most of the online participants are not aware of the consequences of cyber activities. As reflected in the questionnaire, about 70% of the people using the internet lacks adequate knowledge of cybercrimes. The world has faced immense cyber-attacks through various schemes because the governments of those countries failed to make cyber education as part of the educational system. Cyber education will at least help to minimize the occurrence of cybercrimes as most people using the internet will know the basic cyber prevention mechanism.

It is assumed that having trust or ignorance makes people vulnerable to cyber-attack, and to avoid that requires a wider cyber awareness campaign among the public. Most online users do not take cyber threats seriously and lack the expertise on how to protect their personal online information. Junger, Montoya, and Overink indicated in their paper on how internet users' knowledge usually is limited and normally naïve of their online activities[107]. They are ignorant of the fact that the online data might be stolen, get infected, and/or used maliciously. It worth mentioning that cyber education acts like a vaccine that would at least make the crime execution more complicated for cybercriminals.

Creating more and more cyber awareness helps to create caution that might lead to the best cyber hygiene practice that will make internet users learn how to protect

themselves against possible cyber threats. The advancement in technological innovations will continue to increase which suggests that cyber education and awareness should not be stopped, just like we always closed our doors when sleeping. People should be able to lock the security flaws just like how they lock their doors in the cyber ecosystem. The thesis further indicates that cybersecurity and its related courses should be added to the curricula from elementary schools to universities to help boost cyber awareness.

Some school of thought believed cyber education has little effects on the occurrence of cyber-attacks, though it did not necessarily mean that people believed cyber education is not needed. The cyber ecosystem is a fast-growing ecosystem where cybercriminals are always a step ahead of their victims. Cybercriminals are knowledgeable innovators in online communities with malicious intentions that target their victims. This suggests that internet users are always behind one step as that of the cybercriminals. Educating online users only work in institutions where the employees are continuously faced with cybercrime threats. However, it impossible for organizations to safeguard their employees, if they failed to educate them, their data will be in the hands of third parties. This means that they will lose control of their details, with awareness or non-awareness making no difference in fighting cybercrime.

Significance of cyber awareness

The prevailing threats in the cyber ecosystem nowadays are disturbing. Whether the threats are personal or non-personal, normally a certain level of preventive measures is possible to the disturbances of human security in the online ecosystem. The key problem with human security is that people normally do not comprehend the severity of attacks they might be facing daily. People start only to be more cyber cautious when they are been attacked, such as not following the best practice on how to use passwords and other security parameters daily.

Conclusion

The research concludes that there is no legislature to deter cybercrimes at the moment in Sierra Leone. And most of the youths use the internet platform to socialize; such as twitter, Facebook, WhatsApp, Skype, QQ International, and WeChat. Unfortunately, cyberspace is not protected, and many internet subscribers lack the rudimentary skills to protect their personal information. The questionnaire provides awareness of internet crimes and ensures that people take basic security measures to protect their information. Although there are no laws relating to cybersecurity and cybercrime locally, the state has initially created few agencies to deal with such scandalous activities such as; the ONS, the fingerprint department, the ballistic and handwriting department, the cyber unit at the criminal investigation department at the Pa Demba Road, Freetown Sierra Leone. Fortunately, a draft bill is in its initial stage for Parliamentary Approval.

Chapter 8
Conclusion and Recommendations

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

***Corresponding author:** Ibrahim Abdulai Sawaneh, Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone, Email: ciddiisawaneh@hotmail.com

Introduction

This chapter presents the final summary of the whole work and makes several recommendations on how to protect online users. With advances in technological innovations, hackers and online criminals always tricked their victims to steal valuable data.

Conclusion

Security dimensions have changed severely in the last twenty years and several studies have indicated the challenges posed by organizations with regards to cybersecurity and the risks associated with cyber vulnerabilities. Cybersecurity has become a hot research topic in nowadays due to the rampant negative effects and also the introduction of bitcoins used as a medium for making online payment to hackers. Cyber-attacks are on the increase daily due to the continuous advancement in technological innovations. Cybersecurity threats require robust collaboration among states and individual organizations to help combat threats associated with security issues and challenges.

Human factors are viewed as the most frequent security exploit and vulnerability in digital systems. Malicious agents normally invade employee's online activities to find weaknesses. Social media platforms serve as the main source of information where hackers manipulate, defraud online users, and steal their data. A key challenge of the cyberspace is to create user awareness and behavior

on cyber-related issues, as well as on the managerial understanding of cybersecurity characteristics. The latest technological standards with regards to primary security ethics primarily reduce the most risk associated with vulnerabilities in digital systems. However, it is impossible to defend 100% against all security threats. Therefore, the organization must be proactive in detecting and responding to numerous security threats. Malicious users will always bypass the impassive security firewalls to log into the system. Detect and response tools ultimately mitigate the consequences of a cyber-attack, along with the system recovery functions. Furthermore, the data accessed by the hackers can be shared with other organizations, so that they can prepare or adjust to those threats shortly.

Rigid and intense research on cybercrime and cybersecurity-related schemes should be adopted by all nations and individual business entities to prepare them for better and effective security practices. Nations and business entities should enact strong cybersecurity regulations to enhance safer and secure cyberspace. As technology continues to advance, more security threats and challenges are faced by digital entities, thereby making it difficult to align security regulations with modern ways to secure an organization. More cyber education is needed from supervisors to create more cyber awareness among internet users more especially at governmental and business levels. Cyber education may likely prevent cybercrime through though and better cyber practices, even if not completely eradicating such crimes occurring but at least helps to minimize it from happening and subsequently provide a more secure cyber environment. Modern technology through the use of ICT applications and traditional engineering ensures proper security practices among organizations. Incorporating cyber education in high schools, colleges, and university curricula creates a perfect cyber ecosystem where internet users will be able to prevent less advanced cyberattacks occurring on a large scale. This helps improve systems overview and surely enhance better security practices.

Recommendations

Based on the questionnaire issued to respondents, the author was able to analyze and forward some recommendations to help enhance the cyberspace within the confine of Sierra Leone and its surrounding neighbors as indicated below:

1. The government of Sierra Leone through the Ministry of Basic Education, Ministry of Higher and Technical Education and the TEC should develop curricula on cybersecurity studies to be taught from junior secondary schools to universities. This helps create cyber awareness among internet users in the country.
2. The current laws on national security are revised to incorporate challenging laws concerning cybercrimes and cybersecurity threats.
3. The government agencies with the mandate to provide security in Sierra Leone establish advanced forensic laboratories to examine the numerous cybercrimes.
4. Continuous staff developing training programs should be provided internally or externally to broaden staff expertise in handling cybercrimes.
5. A proactive mechanism should be implemented to prevent large-scale cyber-attacks.
6. A national security scheme with the state-of-the-art cybersecurity platform should be established with rigorous security requirement control measures that aim to minimize cybercrimes in Sierra Leone.
7. Implement strict policies that will promote awareness on how cybercrimes hinder the development of all facets of societies.

8. The Anti-Corruption Commission (ACC) should be vigilant in prosecuting cybercriminals and impose huge fines. Furthermore, automating all governmental departments to minimize corruption among the civil servants. Corruption destroys national development and hinders improvement.
9. The government should also allocate grants for colleges and universities to conduct quality research on cybersecurity and its related disciplines. Research helps countries identify potential issues that will drive the development of those countries.
10. All government departments should assign security experts to monitor and prevent cyber-attacks.
11. Companies and other business entities should also be vigorous and pay attention to security threats as it will cost them millions of dollars if their systems fall short of cyber-attacks.

Future Work

As Sierra Leone has embraced science and technology, cybercrime becomes a key element for the government to be vigilant in securing its cyberspace from malicious activities. Ignoring the effects and impacts to fully comprehend the diverse techniques used to protect people's privacy results in the catastrophe that will cost millions of U.S dollars. The researcher recommends the introduction of cyber studies starting from elementary schools to universities to create cyber awareness among the population. Therefore the researcher anticipates conducting further research to unearth more advanced techniques on how to identify and prevent cyber-attacks in post-war Sierra Leone.

Furthermore, due to the restriction made in interviewing cybercriminals at the national headquarters of the CID's cybercrime unit subsequently narrow the research. The researcher also recommends in the future that authorities' concern grant permission to future researchers to identify the various root causes of cybercrimes. Policymakers in the Sierra Leone House of Parliament should revisit the colonial laws and impose huge fines on any mobile and internet companies to protect its clients' data and privacy. Finally, the author further recommends that a wide study be conducted into the demographic and social individuality of cybercriminals in Sierra Leone and discourage factors that influence hackers to commit cybercrime.

References

1. Eriksson, Johan & Giacomello, Giampiero (2006). The Information Revolution, Security, and International Relations: (IR) relevant Theory? International Political Science Review vol. 27: 221-244.
2. Compete for site comparison. http://siteanalytics.compete.com/ facebook.com+myspace.com+twitter.com/
3. C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich et al (2011). Show Me the Money: Characterizing Spam-advertised Revenue. USENIX Security Symposium.
4. B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski et al (2009). Your Botnet is My Botnet: Analysis of a Botnet Takeover. In ACM Conference on Computer and Communications Security (CCS).
5. B. Stone-Gross, T. Holz, G. Stringhini, G. Vigna (2011). The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. In USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET).
6. N. Provos, P. Mavrommatis, M. A. Rajab, F. Monrose (2008). All your iFRAMEs point to Us. In USENIX Security Symposium.
7. C. Grier, K. Thomas, V. Paxson, M. Zhang (2010). @spam: the underground on 140 characters or less. In ACM Conference on Computer and Communications Security (CCS).
8. K. Thomas, D. McCoy, C. Grier, A. Kolcz, V. Paxson (2013). Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. In USENIX Security Symposium.
9. Trends in World Military Expenditure, 2017" (PDF). Stockholm International Peace Research Institute.
10. "Data for all countries from 1988-2017 in constant (2016) USD (pdf)" (PDF). SIPRI.
11. Dunn M (2003). Securing the Digital Age. In Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security, ed. Robert Latham. New York: The New Press 85-105.
12. c5franey. (2011). Disaster Recovery Plan. Retrieved March 21, 2012, from Study Mode: http://www.studymode.com/essays/Disaster-Recovery-Plan-809693.html
13. T. Jagatic, N. Johnson, M. Jakobsson, T. Jagatif (2007). Social phishing. Communications of the ACM.
14. L. Bilge, T. Strufe, D. Balzarotti, E. Kirda (2009). All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. World Wide Web Conference (WWW).
15. G. Stringhini, O. Hohlfeld, C. Kruegel, G. Vigna (2014). The harvester, the botmaster, and the spammer: On the relations between the different actors in the spam landscape. In ACM Symposium on Information, Computer and Communications Security (ASIACCS).
16. Lewis, James A. (2014). "National Perceptions of Cyber Threats". Strategic Analysis 38: 4.
17. Ibid 567.
18. Singer & Friedman 39.
19. Visit report, Sierra Leone Security and Intelligence Service Reform 1999.
20. Buzan, B, Hansen, L. (2009). The Evolution of International Security Studies, Cambridge University Press, Cambridge.

21. Yost, David (2010). NATO's evolving purposes and the next Strategic Concept. International Affairs 86: 489 -522.

22. http://www.nato.int/summit2009/topics_en/21-nato-eu_strategic_partnership.html

23. NATO (2016). NATO Defence Ministers Agree to enhance collective and deterrence. Last accessed 14.7.16 from http://nato.int/cps/en/natohq/news 132356.html? Selected Locale=en.

24. Singer, Peter, Friedman, Allan (2014). Cybersecurity and Cyberwar. Oxford University Press.

25. Clarke, Richard (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: Harpers Collins.

26. Lewis, James Andrew. 2016. Managing Risk for the Internet of Things. Center for Strategic and International Studies. February. http://csis.org/files/publication/160217_Lewis_ ManagingRiskIoT_Web_Redated. pdf.

27. Kieler, Ashlee. 2014. Study Confirms That Most Of Us Carry Less Than $50 Cash. Consumerist. May 12. http://consumerist.com/2014/05/12/study-confirms-thatmost-of-us-carry-less-than-50-cash/.

28. World Economic Forum. 2016. Hyper-connected World. https://www.weforum.org/global-challenges/projects/hyperconnected-world.

29. United Nations. 2016. Cybersecurity Demands Global Approach. http://www.un.org/en/ development/desa/news/ecosoc/cybersecurity-demandsglobal-approach.html.

30. Norton. 2016. Phishing. http://us.norton.com/security_response/phishing.jsp.

31. Clapper, James. 2016. Statement for the Record, Director of National Intelligence, James R. Clapper, Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee. February 9. http://www.armedservices.senate.gov/imo/media/doc/ Clapper_02-09-16.pdf.

32. 2015. Remarks by President Obama and President Xi of the People's Republic of China in the Joint Press Conference. September 25. https://www.whitehouse.gov/thepress-office/2015/09/25/remarks-president-obama-and-president-xi-peoplesrepublic-china-joint.

33. Ferdinando, Lisa 2014. Cyberspace Chief: Beware the Adversary is Watching. The U.S. Army 3.

34. http://www.army.mil/article/133011/Cyberspace_chief__Beware__the_adversary_is watching/.

35. Gibbs, Samuel. 2014. FBI: 90% of US Companies Could Be Hacked Just Like Sony. The Guardian. December 12. http://www.businessinsider.com/fbi-90-of-cybersecurity-systems-out-there-would-not-have-been-able-to-block-the-sony-hackers2014-12.

36. Department of Defense. 2016. Department of Defense Releases Fiscal Year 2017 President's Budget Proposal. February 9.http://www.defense.gov/News/NewsReleases/News-Release View/Article/652687/department-of-defense-dod releases-fiscal-year-2017-presidents-budget-proposal. Accessed 2016.

37. Bug crowd. 2016. The Bug Bounty List. https://bugcrowd.com/list-of-bug-bountyprograms. Accessed.

38. Facebook Company Info. 2016. http://newsroom.fb.com/company-info/. Accessed.

39. Finkle, Jim. 2016. Apple users targeted in first known Mac ransomware campaign. Reuters. March 6. http://www.reuters.com/article/us-apple-ransomwareidUSKCN0W80VX. Accessed.

40. Crouch, Angie. 2016. Hollywood Hospital 'Victim of Cyber Attack'. NBC Los Angeles. February 2. http://www.nbclosangeles.com/news/local/Hollywood-HospitalVictim-of-Cyber-Attack-368574071.html. Accessed.

41. Hiltzik, Michael. 2016. 2016 is shaping up as the year of ransomware -- and the FBI isn't helping. Los Angeles Times. March 8. http://www.latimes.com/business/hiltzik/lafi-mh-2016-is-the-year-of-ransomware-20160308-column.html. Accessed.

42. Director of National Intelligence. 2015. Remarks as delivered by the Director of National Intelligence, James R. Clapper. January 7. http://www.dni.gov/index.php/newsroom/speeches-and-interviews/208-speechesinterviews-2015/1156-remarks-as-delivered-by-dni-james-r-clapper-on%E2%80%9Cnational-intelligence,-north-korea,-and-the-national-cyberdiscussion%E2%80%9D-at-the-international-con. Accessed.

43. Yoder, Eric. 2016. Official overseeing breached OPM computer systems retire just ahead of House hearing. The Washington Post. February 22. https://www.washingtonpost.com/news/powerpost/wp/2016/02/22/officialoverseeing-breached-opm-computer-systems-retires-just-ahead-of-house-hearing. Accessed.

44. Nakashima, Ellen. 2013. The confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. The Washington Post. May 27. https://www.washingtonpost.com/world/national-security/confidential-reportlists-us-weapons-system-designs-compromise bychinesecyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b 0b5e9247e8ca_story.html?tid=a_inl. Accessed.

45. Weisgerber, Marcus. 2015. China's Copycat Jet Raises Questions about F-35. Defense One. September 23. http://www.defenseone.com/threats/2015/09/more-questionsf-35-after-new-specs-chinas-copycat/121859/. Accessed.

46. Boykoff, Pamela. 2015. China denies suggestions it stole designs for new U.S. fighter. CNN. January 20. http://www.cnn.com/2015/01/19/world/china-us-f35-fighterdenial/. Accessed.

47. FBI. 2016. Cyber's Most Wanted. https://www.fbi.gov/wanted/cyber. Accessed.

48. Department of Justice. 2014. U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. https://www.justice.gov/opa/pr/us-charges-five-chinesemilitary-hackers-cyber-espionage-against-us-corporations-and-labor. Accessed.

49. Cloherty, Jack, and Pierre Thomas. 2014. Trojan Horse Bug Lurking in Vital US Computers since 2011. ABC News. November 6. http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers2011/story?id=26737476. Accessed.

50. Clarke, Richard. 2010. Cyber War: The Next Threat to National Security and What to Do about It. New York: Harpers Collins.

51. Pagliery, Jose. 2016. Scary questions in Ukraine energy grid hack. CNN Money. January 18. http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/. Accessed.

52. Perez, Evan. 2015. How the U.S. thinks Russians hacked the White House. CNN. April 8. http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/. Accessed.

53. Winter, Michael. 2014. Report: Iran hacking key U.S., global firms. USA Today. December 2. http://www.usatoday.com/story/news/world/2014/12/02/iranhackers-infiltrate-energy-transport infrastructure/19806247. Accessed.

54. Gorman, Siobhan. 2014. Navy Hacking Blamed on Iran Tied to H-P Contract. Wall Street Journal. March 5. http://www.wsj.com/articles/SB10001424052702304732804579423611224344876. Accessed.

55. Yadron, Danny. 2015. Iranian Hackers Infiltrated New York Dam in 2013. The Wall Street Journal. December 20. http://www.wsj.com/articles/iranian-hackersinfiltrated-new-york-dam-in-2013-1450662559. Accessed.

56. Park, Ju-Min, and James Pearson. 2014. In North Korea, hackers are a handpicked, pampered elite. Reuters. December 5. http://www.reuters.com/article/us-sonycybersecurity-northkorea-idUSKCN0JJ08B20141205. Accessed.

57. Perez, Evan. 2015. How the U.S. thinks Russians hacked the White House. CNN. April 8. http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/. Accessed.

58. Winter, Michael. 2014. Report: Iran hacking key U.S., global firms. USA Today. December 2. http://www.usatoday.com/story/news/world/2014/12/02/iranhackers-infiltrate-energy-transport-infrastructure/19806247. Accessed.

59. Gorman, Siobhan. 2014. Navy Hacking Blamed on Iran Tied to H-P Contract. Wall Street Journal. March 5. http://www.wsj.com/articles/SB10001424052702304732804579423611224344876. Accessed.

60. Yadron, Danny. 2015. Iranian Hackers Infiltrated New York Dam in 2013. The Wall Street Journal. December 20. http://www.wsj.com/articles/iranian-hackersinfiltrated-new-york-dam-in-2013-1450662559. Accessed.

61. Park, Ju-Min, and James Pearson. 2014. In North Korea, hackers are a handpicked, pampered elite. Reuters. December 5. http://www.reuters.com/article/us-sonycybersecurity-northkorea-idUSKCN0JJ08B20141205. Accessed.

62. http://www.mynewsdesk.com/uk/virgintrains/pressreleases/new-azuma-trains-arrive-at-uk-port-ahead-of-passenger-services-starting-later-this-year-2453824.

63. Ashton, K. 2009. That 'Internet of Things' Thing, RFID Journal. Retrieved from http://www.rfidjournal.com/articles/view?4986.

64. Gartner. 2017. Gartner Says 8.4 Billion Connected "Things" Will Be in Use 2017, Up 31 Percent From 2016. Retrieved from https://www.gartner.com/newsroom/id/3598917.

65. Tarkoma, S. 2017. The Internet of Things Research Program and Beyond. IoT Security Workshop 07.09.2017 in Aalto University. https://www.vahtiohje.fi/web/guest/vm-vahti-ja-tietoturvallisuus.

66. Amara A Samura (2019). Legislate Cyber Laws. New Vision Newspaper1 & 3.

67. Mohamed Sankoh (2019). NATCOM and Civil Rights Coalition on Cyber Security Sensitization. Unity Newspaper 69: 9.

68. Ade Campbell (2019). Information Ministry Looks at Cyber Security. Awoko Newspaper 56: 6.

69. "What I Talk About When I Talk About Platforms". Martinfowler.com. Retrieved 2019-04-28.

70. "Platforms". Free On-line Dictionary of Computing. Retrieved 2019-04-28.

71. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/Hacker_cracker_attacker.pdf. Retrieved 2019-04-28.

72. "Internet Users' Glossary". Archived from the original on 2016 -0-05. RFC 1983. Retrieved 2019-04-28.

73. E. Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: Achievements and next steps: towards global cyber-security" 2011.

74. Stephen Gandel, "Lloyd's CEO: Cyber-attacks cost companies $400 billion every year", http://fortune.com/2015/01/23/cyber attack-insurance-lloyds/

75. Alan Tovey, “Average cost of cyber-attacks doubles to £1.46m”, Telegraph Financial News Online, http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/11646347/Average-cost-of-cyber attacks-doubles-to-1.46m.html

76. Mahmoud Khonji, Youssef Iraqi, and Andrew Jones, “Mitigation of Spear Phishing Attacks: A Content-based Authorship Identification Framework”, Proceedings of the 6th International Conference for Internet Technology and Secured Transactions (ICITST) 416-421.

77. Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H. Raghav Rao, “Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email”, IEEE Transactions on Professional Communication 55: 345-362.

78. “Understanding Denial - of - Service Attacks”. US-CERT. 6 February 2013. Retrieved 2019.

79. For a good introduction to the subject of botnets, see Ramneek Puri, “Bots & Botnet: An Overview.”, SANS Institute, 8 August 2003, http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299.

80. Prince, Mathew (2016). “Empty DDoS Threats: Meet the Armada Collective”. Cloudflare. Retrieved.

81. “Brand.com President Mike Zammuto Reveals Blackmail Attempt” 2014. Archived from the original.

82. “Brand.com’s Mike Zammuto Discusses Meetup.com Extortion”. 5 March 2014. Archived from the original.

83. Romagna M, Van Den Hout N. J (2017). “Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats”. Proceedings of the 27th Virus Bulletin International Conference: 41 - 50. Retrieved.

84. My colleague Thomas Steinbrenner once explain SQL injection in the following way: “Computers know two things: instructions and data. Simply speaking, an SQL injection is when the computer expects data as input but you provide instructions instead and trick it into executing them.”

85. https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf

86. In 2017, cybercrime costs accelerated with organizations spending nearly 23 percent more than 2016 - on average about $11.7 million. https://www.varonis.com/blog/cybersecurity-statistics/ via @varonis.

87. The Cost of Cyber Crime Study. https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017?src=SOMS.

88. The Cost of Cyber Crime Study. https://www.accenture.com/us-en/event-cybertech-europe-2017?src=SOMS#block-insights-and-innovation.

89. The Cost of Cyber Crime Study. https://www.accenture.com/us-en/event-cybertech-europe-2017?src=SOMS#block-insights-and-innovation.

90. Top cybersecurity facts, figures and statistics for 2018. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

91. Cybersecurity Ventures Official Annual Cybercrime Report. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

92. http”//www.twitter.com/somcumuns

93. Beyond hashtags: how a new wave of digital activists is changing society. https://theconversation.com/beyond-hashtags-how-a-new-wave-of-digital-activists-is-changing-society-57502 Rid 2012, 20.

94. Ex-CIA agent Jerry Chun Shing Lee admits spying for China. http://www.bbc.com/news/world-us-canada-48130068.

95. Aven T (2015). Risk analysis, 2nd edition, John Wiley & Sons.

96. Taleb, N. N (2007). The Black Swan - the impact of the highly improbable. United States: Random House.

97. Aven T, Krohn, B.S (2014). A New Perspective on how to Understand, Assess and Manage Risk and The Unforeseen from Reliability Engineering and System Safety Elsevier.

98. https://www.itgovernance.co.uk/cyber-security-risk-assessments. Accessed June 2, 2019.

99. Marinos, L., Belmonte, A., Rekleitis, E., 2016. ENISA Threat Landscape 2015. [pdf] Available at: https://www.enisa.europa.eu/publications/etl2015.

100. Marinos, L., 2014. ENISA Threat Landscape 2014. [pdf] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014.

101. "Peddler's martyrdom launched Tunisia's revolution: Reuters.

102. "Uprisings in the region and ignored indictors" Payvand.

103. Lloyd's, 2010. Digital Risk Report - Managing Digital Risk. [pdf] Available at: https://www.lloyds.com/~/media/lloyds/reports/360/360-digital/lloyds_360_digital_risk_report-(2).pdf[Accessed 03.06.2019]

104. Kargbo A. B. (2019). Mobile Phone Operators on Massive Registration Exercise. War against Cyber Crime, Standard Times 83: 7.

105. Samura A. A. 2019. WAEC Fraudsters, Standard Times 83: 7.

106. Bah M. J. 2019. Financial Intelligence Unit to Combat Money Laundering and Terrorism Financing, Awoko Newspaper 25: 2.

107. Breaking down Cyber Basics: Understanding Vulnerabilities, Threats & Exploits at https://www.bitsight.com/blog/breaking-down-cyber-basics-understanding-vulnerabilities-threats-exploits

108. Human factors Working Group White Paper: https://pdfs.semanticscholar.org/38b4/36a07f78056a82df1e9228b87ca145f09f9c.pdf

109. Junger, Marianne, Lorena Montoya, F.J. Overink (2017). "Priming and warnings are not effective to prevent social engineering attacks". Computers in Human Behavior 66.

Appendix I Research Questionnaire

General Information

Organization Name: ……

……..

Address of the Organization:……..

……

Organizational website: ……..

Email Address of the Participant: ……

Name of the Participant: ……

Description of the agency's operations: ……

……

……

Effective Management Policy

1. Do key position requires any pre-requisite qualification in the state security force?

Yes ☐ No ☐

2. Are there any backup policies for recording sensitive state documentation?

Yes ☐ No ☐

3. Do the backup personnel have the required skill to handle such position?

Yes ☐ No ☐

4. Is there any law(s) binding the telecommunication service provider(s) to disclose any security threats ether to the state or individual people to the state security forces?

Yes ☐ No ☐

If no, what will be the Plan B approach?

……

……

……

5. Are there any IT audit system that examines the effectiveness of organization's cyber security policies, procedures and controls?

Yes ☐ No ☐

6. How often, if there is any one, do employees attend training/workshop/seminar on how to passwords should be strengthening and change regularly?

Yes ☐ No ☐

7. Do the government of Sierra Leone provide enhancement training in cyber security internally or externally?

Yes ☐ No ☐

8. How often is security testing is done in Sierra Leone?

Annually ☐ Bi Annually ☐ Quarterly ☐

9. Do employees disclose sensitive or confidential information to third party without proper authorization?

Yes ☐ No ☐

10. Do staff, including top management, discusses or disclose sensitive or confidential information with family and friends off work?

Yes ☐ No ☐

11. Do the agency have any backup and recovery plan from a virtual system?

Yes ☐ No ☐

12. Is there any life insurance in place for senior management? ☐

Yes ☐ No ☐

13. Does the agency ensure complicate and / or strong password policies are in place as a mandatory to all staff that is changed at a time interval?

- ☐ Yes, a mandatory password change regularly
- ☐ Yes, does not requires a mandatory password change at a time interval
- ☐ No

14. Is there any disaster recovery plan in your agency or department?

Yes ☐ No ☐

15. How do the collected data saved in your department?

- ☐ A physical server at a known location in the office.
- ☐ Saved on the cloud server hosted by cloud service providers.
- ☐ Save on external storage devices (External Hard Drive, flash drive etc.)
- ☐ Saved ordinarily on the office desktop computer.

16. Does the agency have a comprehensive framework of facilities, systems and procedures that allow for continued dangerous operations when large numbers of staff are not on duty for a period of time?

Yes ☐ No ☐

Physical Security Features

17. Are there any CCTV cameras installed to observe staff activities in the agency or various departments? if yes how?

Yes ☐ No ☐

If yes ……

……..

18. Are there any ATM within the agency's premises?

Yes ☐

No ☐

Not applicable ☐

19. Are there any regulations on how outdated hard drives, CDs, flash drives or any other storage medium destroyed or retired according to approved policies and procedures?

Yes ☐ No ☐

20. How does the agency or department handle privacy issues?

- ☐ They have policies that regulates such issue.
- ☐ Do not pay attention to such issue.
- ☐ They do not have any policy relating to privacy issue.

21. Are privacy screens installed on monitors in public areas and/or are monitors situated in such a way that is not viewed by unauthorized individuals?

Yes ☐ No ☐

22. Are there any awareness on social engineering and agency's plans featured in the security-training program?

Yes ☐ No ☐

23. Are the internal hard drives in copiers, printers, and multifunction peripheral devices destroyed or retired according to approved policies and procedures?

Yes ☐ No ☐

24. Do the agency's desktops and laptops secured via locking cable or anti-theft device?

Yes ☐ No ☐

25. Do the agency make it a mandatory to all financial institutions to install CCTV cameras on each ATM machines nationwide?

Yes ☐ No ☐

26. Is there any policy on how to deal with bomb, hostage or terrorist threat?

Yes ☐ No ☐

27. Does the agency server room have any temperature sensor the monitor the room?

Yes ☐ No ☐

28. Does the agency have the necessary hardware and software to handle cybercrime monitoring?

- ☐ Yes, but most are outdated
- ☐ Yes, with the recent development
- ☐ No

29. Do the agency outsource any services from other entities? If yes, kindly state the service(s).

Yes ☐ No ☐

30. Is there any forensic laboratory to investigate cybercrime activities in Sierra Leone?

Yes ☐ No ☐

31. Does the agency have any firewall installed on the servers?

Yes ☐ No ☐

Logical Security

32. Which types of Network infrastructure do the agency/department has?

……

……

33. Does network changes application documents?

Yes ☐ No ☐

34. Do all the virtual systems comply with the applicable security policies?

Yes ☐ No ☐

35. Do individual staff logoff their workstations when they away from the desk?

Yes ☐ No ☐

36. Do the agency permits to individual user to act as a local administrator on the agency's computers?

Yes ☐ No ☐

37. Does the agency have any formal process for applying computer and application patches?

Yes ☐ No ☐ Not Applicable ☐

38. Are the state security apparatus trained to identify a legitimate warning message from a scam message that could result in downloading a virus?

Yes ☐ No ☐

39. Do the agency have any policy on staff bring their own devices to work?

Yes ☐ No ☐

40. Do the agency grant access to third parties including vendors?

Yes ☐ No ☐

41. Is there any policy as to encrypt backup documents?

Yes ☐ No ☐

42. If accesses are granted to third party, will the agency terminate the service after the time elapse?

Yes ☐ No ☐

43. Does the agency have a process for intrusion detection and are employees trained to monitor intrusion properly?

Yes ☐ No ☐

44. Are there any policies on the following?

Networking Security Policy	Yes ☐	No ☐
Privacy Security	Yes ☐	No ☐
Identity Theft Prevention Policy	Yes ☐	No ☐
Breach Incident Response Policy	Yes ☐	No ☐
Disaster Recovery Policy	Yes ☐	No ☐

Laptop/Computer Utilization Policy	Yes	☐	No	☐
Confidentiality	Yes	☐	No	☐

45. Is there any Ant-Virus protection system in the agency?

Yes ☐ No ☐

46. Is there any policy instructing your agency to delete or remove offensive comment especially on social media

Yes ☐ No ☐

Declaration

The respondent confirms that all the statements made above are true and correct to the best of his/her knowledge.

Signature of the Researcher: …… Date: ……..

Signature of the Respondent: …… Date: ……..

Appendix II Doctoral Publications

This section throws insights onto a few articles published during the Doctoral Degree academic struggle. It shows that the author conducted extensive research to fulfill the academic requirements for the award of Ph.D. Degree in Computer Science at the Atlantic International University in the U.S

List of Doctoral Publications

Table A1 indicates the articles published during the doctoral research by the author.

Selected Publications		
Journal	**Title**	**Other Details**
European Journal of Computer Science and Information Technology	The Role of Cyber Security in Minimizing Crime Rate in Post-War Sierra Leone	Pp. 36 - 47, Vol. 7, N0. 2, April 2019. www.eajournals.org
International Journal of Precious Engineering Research and Applications (IJPERA)	Cyber Security and Its Challenges posed by Latest Technologies in Post - Ebola Sierra Leone	Pp. 20 - 28, Vol. 4, Issue 2, March - April 2019. www.ijpera.com
International Journal of Intelligent Information Systems	Examining the Effects and Challenges of Cyber Security within the Cyberspace in Sierra Leone	Pp. 23 - 27, Vol. 7, Issue 3, October 2018. http://www.sciencepublishinggroup.com/j/ijiis DOI: 10.11648/j.ijiis.20180703.11
International Journal of Precious Engineering Research and Applications (IJPERA)	Cyber Security and Its Challenges posed by Latest Technologies in Post - Ebola Sierra Leone	Pp. 20 - 28, Vol. 4, Issue 2, March - April 2019. www.ijpera.com

Other Publications

Table A2 states other publications done from 2017 to August 2019.

Other Publications			
No.	**Journal**	**Title**	**Other Details**
1.	International Journal of Medical Imaging	An Effective Method for e-Medical Data Compression using Wavelet Analysis	Pp. 25 - 32, Vol. 6, Issue 3, December 20, 2018. http://www.sciencepublishinggroup.com/j/ijmi DOI: 10.11648/j.ijmi.20180603.12
2.	International Journal on Data Science and Technology	Student Dissertation Database Management System: IMATECH Sierra Leone as a Case Study	Pp. 93 - 99, Vol. 4, Issue 3, October 25, 2018. http://www.sciencepublishinggroup.com/j/ijdst DOI: 10.11648/j.ijdst.20180403.13
3.	IEEE	A survey on security issues and wearable sensors in wireless body area network for healthcare system.	978 - 1 - 5386 - 1010 - 7/17/$31.00 © 2017 IEEE Pp. 304 - 308
4.	International Journal of Computer Science and Mobile Computing	Medical Image Denoising and Compression via a 2-D Wavelet Transform	Pp. 23 - 30, Vol. 7, Issue 6, June 2018. www.ijcsmc.com
5.	International Journal of Interdisciplinary Research and Innovations	Application of Discrete Wavelet Transform for Compressing Medical Image	Pp. 471 - 475, Vol. 6, Issue 2, April - June 2018. www.researchpublish.com
6.	International Journal of Computer Science and Information Technology Research	A Computerized Patient's Database Management System	Pp. 6 - 10, Vol. 6, Issue 2, April - June 2018. www.researchpublish.com
7.	Journal of Advanced Research in Medical & Health Sciences	DWT Based Image Compression for Health Systems	Pp. 1- 67, Vol. 4, Issue 9, Sept. 2018
8.	International Journal of Scientific Research and Management	An Assessment of the Effectiveness of Performance Appraisal System in Educational Institution: IAMTECH Sierra Leone as a Case Study	Pp. 203 -209, Vol. 6, Issue 6, DOI: 10.18535/ijsrm/v6i6.sh05. www.ijsrm.in

9.	European Journal of Human Resource Management Studies	Assessing Employees' Motivation in Tertiary Educational Institutions in Sierra Leone: Institute of Advanced Management and Technology & Njala University	Pp. 24 - 36, Vol. 2, Issue 1, 2018. DOI: 10.5281/zenodo.1464277. http://www.oapub.org/soc
10.	International Journal of Social Sciences and Humanities Research	Financial Management in Party Politics to Enhance Sustainable Development in Developing Nations	Pp. 1 - 5, Vol. 6, Issue 2, April - June 2018. www.researchpublish.com
11.	Journal of Human Resource Management	An Effective Employee Retention Policies as a way to boost Organizational Performance.	Pp. 41 - 48, Vol. 7, No. 2, July 13, 2019. DOI: 10.11648/j. jhrm 20190702.12. http://www. sciencepublishinggroup.com/j/jhrm
12.	Science Journal of Business and Management	Evaluating Employee Retention Strategies on Job Performance	Pending
13.		An Assessment of the Effectiveness of Performance Appraisal in Educational Institution: A Case Study of the Institute of Advanced Management and Technology (IAMTECH): Thesis publication - (Thesis)	Pending

About the Author

Ing Ibrahim Abdulai Sawaneh, Former Director of Academic Affairs at the Institute of Advanced Management and Technology (IAMTECH) - Sierra Leone. He is currently a lecturer at the Ernest Bai Koroma University of Technology - Sierra Leone. He is also the Director of Quality Assurance at IAMTECH. He has authored few textbooks and done several journal publications in recognized international journals.

ISBN: 978-1-63278-972-3

978-1-63278-972-3