ISSN 2319-1236

Cyber Security Education: A Tool for National Security

Morufu Olalere, Dr. Victor O. Waziri, Idris Ismaila, Olawale S. Adebayo, Joel N. Ugwu

Cyber Security Science Dept., FUTMINNA, Nigeria

lerejide@futminna.edu.ng

HOD, Cyber Security Science, Dept., FUTMINNA, Nigeria

Onomzavictor@gmail.com

Cyber Security Science Dept., FUTMINNA, Nigeria

ismi_idris@yahoo.co.uk

Cyber Security Science Dept., FUTMINNA, Nigeria

waleadebayo@futminna.edu.ng

Cyber Security Science Dept., FUTMINNA, Nigeria

Joel.ugwu@st.futminna.edu.ng

ABSTRACT

The rate at which cybercrime is being perpetrated in our society is quietly alarming, the insecurity of internet has exposed the global community and resources to this menace, many nations, organizations and individuals are becoming victims of this on daily basis. Many Individuals have lost their personal information into the hands of hackers, it is now easy for people to masquerade the identity of others, organizations lose edge to their competitors as their confidential information have been revealed, many nations are engaged in cyber war against the other, all these activities are being perpetrated on the cyberspace. As a result of these, this paper seeks to highlight the impact of cyber security education on national security by identifying its importance, to both individual and organizations and to the nation at large. We suggest introduction of Cyber Security education into the curriculum of primary and basic eduction of any nation.

Indexing terms/Keywords

Cybercrime; Cyberspace; Cyber Security; Cyber Security Education; Attack.

Academic Discipline And Sub-Disciplines

Information and communication Techology/Cyber Security Science

SUBJECT CLASSIFICATION

Information security

TYPE (METHOD/APPROACH)

Theoretical

INTRODUCTION

The effect of cybercrime to organization is devastating, hackers use sophisticated software tools to leverage vulnerabilities and threat to attack individuals, organizations, or countries for various reasons, including financial gains, business disruption or political purposes. These attacks seem to have been on increase since the inception of internet which has brought a revolutionized mode of communication making the world a global village.

The internet network has brought so many possibilities into the modern methods of communication, it is now possible to transfer data files across cities within a few seconds, people can hear each others` voice using Internet Protocol calls, organizations can collaborate more effectively and even centralize their transactions, there can even be e-Business, e-Education, e-Health, and e-Government. All these seek to better the life of citizenry and bring basic human needs closer at ease.

The ease of communication brought by the use of internet has brought so many developments to many activities of mankind, and as well brought new dimension of security challenges. For instance, as it is easy for one to perform online transactions like buying of goods and money transfer anywhere, it is also possible for hackers to obtain victim transaction identities and passwords in clear text through the network you are connected to; The use of electronic mail in our present society is successfully phasing out the traditional method of letter writing, hackers can successfully obtain your email address and password by sending a mail containing malicious code(such as root kit or Trojan) which can run as a script and send back the required information to the hacker.

National security could be seen as the protection or the safety of country`s secrets and its citizens (Macmillan Dictionary; Online version). Emphasizing on the term, Senator Ike Eweremadu on his public lecture titled “Policing and National Security in Nigeria: The Choices before Us” delivered at Nnamdi Azikiwe University, Awka, Nigeria defined national security as “all that the state and citizens do, from individual to institutional level, to ensure security of lives and property” (ThisdayLive, 2013). From these points, we could infer that a nation is said to be secure when its information and resources are free from any forms of threat.

Most Cybercrimes prey on the ignorant and unconsciousness of the user, poor awareness of cybercrime, under-development of policies by some organization, neglects and poor implementations of policies and technical security features by managements in organizations, poor deployment of physical security gadgets, and misuse of security features by the security personnel and poor governmental supports in formulating laws against cybercrime. All these bring about vulnerabilities which attacker exploits to carry out attack on either individual, organization or nation. These vulnerabilities that could result in loss of a valuable property by the individual, organization or even the government if exploited, is mostly left open due to the poor knowledge about the effect of cybercrime on critical infrastructures and society at large. Cyber security education is an essential tool that brings to our consciousness the effect of these cybercrimes and as well informs us of the latest strategies that could be employed to avert the menace of these effects and even expose the users and policy makers to the need for having effective cyber security strategies.

This study highlights the benefits of cyber security education to individuals, organizations and nation at large. It discusses the importance of cybersecurity education as regards to the use of internet, and mobile telecommunication technologies and devices, which are invariably the latest means of communication in our present day society. It begins with its introduction portraying the reason for the research, discussing the concept of cybercrime and cyber security, cyber security education; it also highlighted the impacts on individuals, organizations as well as a nation, and finally conclusion.

CYBERCRIME AND CYBER SECURITY

Cybercrime could be defined as any activity in which computers or networks are used as a tool, a target or a place of criminal activities (ITU-D ICT). These activities could take advantage of weaknesses that exist in the system which can be called system vulnerability. System vulnerabilities varies with state of the system, whether it is in a stand-alone environment where it is not connected to any other device or system, Local Area Network (LAN) environment where it is only connected to a few other computer systems and devices, or in an internet network environment where it is connected to the global computers and devices. A computer connected to global internet network possesses higher proximity to exploit, as its vulnerabilities can be accessed from any part of the world, and also due to the insecurity of internet. Most of the computers and devices that are used for business transactions by organizations and individuals are connected to internet. Many other activities of hackers on this global internet also endanger the information on the computer system or devices that are connected to it. For instance, a hacker can send a bulk SMS masquerading as a legitimate bank, demanding customers to send their transactions` details to a particular telephone number or email address for upgrade. Internet is a pool that harbors both good and bad. Local Area Network (LAN) on the other hand still have some level of insecurity than stand-alone computer, people on the same LAN environment can access each others` file, depending on the level of access privilege the individual possesses on the network. Privilege defines the right of an individual or group to an operation in a given network environment which are being apportioned based on priorities and applicability. A privilege can be denied, or elevated which can be generally termed as violation of privilege. Violation of privileges is a major crime that is perpetrated on local area network, the unsatisfactory human nature terms to show-off itself as individuals try to possess unlimited privilege or a person possessing higher privilege can deny another user the right to some certain operation thereby limiting his access privilege in a network. This particular crime often occur in an organizations like banks, parastatals, ministries, etc. there can also be easy transfer of exploit payloads like rootkits, worms, etc., in a local area network environment.

While a stand-alone computer possess the most minimal proximity to these menace but still have to some extent, certain level of vulnerability. Stand-alone computer can be attacked by physical security, whereby the computer system itself might be stolen or damaged. In a stand-alone environment, off-line cracking of passwords can be possible; it is also possible to destroy files and data with temporary storage devices, like: flash drive, floppy disk, etc. all these vulnerabilities can be exploited constituting crime against stand-alone environment.

The entire network of particular organization can also be attacked; these attacks may be physical or logical. The physical attack might result in destruction of network infrastructures, such as: router, switch, network cables, etc. while the logical attack can result in slowing the connectivity or reduction of network bandwidth. The logical network attack can be very dangerous as the physical network attack as tools can be used to enforce Denial of Service (DoS) and or Distributed Denial of Service (DDoS).

Cybercrime includes a wide variety of crimes (Sieber, 2005). Recognized crime also encompasses a broad range of offences, which also makes it difficult to classify cybercrime (Gordon et al 2006) (Chawki, 2005). An interesting classification system could be found in Council of Europe Convention on Cybercrime, which distinguishes between four different types of cybercrime (ITU-GCA, 2008). They are:

i. Offences against the confidentiality, integrity, and availability of computer data and system;

ii. Computer-related offences;

iii. Content-related offences; and

iv. Copyright-related offences;

The impact of cyber crime on individual, organization and nation cannot be quantified easily. The financial losses caused by cybercrime and the number of offences, are very difficult to estimate (Walden, 2006).

Cybersecurity is an essential security aspect that involves protection of critical information and network infrastructures. It could be defines as the term used to summarize various activities such as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user`s assets (ITU-CLR, 2009). Making the internet safer and protecting the internet users are essential development of new services as well as governmental policy (ITU-WTSAR, 2008). Cybersecurity can sometimes be called IT Security, a field that covers all mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. IT experts do apply some techniques to ensure the security of a system and network (WikiCS, 2009). Some of those techniques are:

i. The techniques of Least Privilege- this ensures that every part of the system enjoys the privilege that are needed for its specific function.

ii. The techniques of Code Review and Unit Testing- this is applied to developed software to ensure that the modules are more secure where formal correctness proof is not possible.

iii. The techniques of Audit Trails – this is used to ensure that system activities are tracked so that when security breaches occur, the mechanism can determine the extent of the breach,

iv. The techniques of defense in depth - this is an information assurance concept in which multiple layers of security controls are placed throughout an information technology (IT) system.

CYBER SECURITY EDUCATION

We define Cyber security Education as the type of education that brings to the knowledge of citizens, organizations, and nation the existence of cybercrime, cyber threats, vulnerability, as well as exposes them to the necessary steps that can be taken to avert its occurrence and also to minimize its risk to an acceptable degree. Cybersecurity education awakens the consciousness of man on the menace of cybercrime; it equips the citizenry on the knowledge about the modern means of communication, and ways of making safe internet transactions especially to non technical users. Cyber security education should be considered integrated into primary and basic education curriculum as it is now an emerging challenge to the nations. Everybody now has email address, even children make use of telephone, many organizations now only base their businesses online, we are now on cashless society whereby some transactions are encouraged to be done online, all these are necessary reasons by which Cyber security education should be integrated into our primary and basic education curriculum so that before adult stage, our children must have known all the cyber tricks and should be knowledgeable enough to avoid being victim of cyber fraud and carry out e-transactions safely. Cybersecurity education also helps us to know the various risks associated with mobile transactions, e-transaction, mobile banking, ATM transactions, POS terminals use, internet transactions, e-Business, e-commerce, e-health, e-education, e-environment, as well as advices us on how to make use of our personal computers and mobile devices safely in both private and public networks. Cyber security education should be seen as a tool that averts the menace of cybercrimes and attack. It fosters good relationship and trust between one individual and another, individual and organization, one organization and another, organization and a nation, as well as one nation and another. Many nations have formulated o means by which this education is being passed, for instance, in United States, October 2010 Cybersecurity month, was dedicated to raising Cybersecurity awareness, and empowering citizens, businesses, government and schools to improve their Cybersecurity preparedness and to promote safe internet experience (Multi-state Information Sharing and Analysis Center (MS-ISAC), 2010). The issue of Cyber security should be taken serious as it has an acute implication on security of personal

information, transactions and money. Organization should also be on-page on the latest strategies of cyber threat, in other to help them secure their confidential information and that of their customers. Organizations should have a dedicated department that has the responsibility of formulating Cybersecurity policy, supervise and ensure the implementation of such policy within that organization as well as educate and train the non technical member of the organization and their customers on how to abide by the policy.

IMPACT OF CYBER SECURITY EDUCATION ON INDIVIDUAL

The impact of Cyber security education on individual cannot be over emphasized; it makes an individual to be aware of the present state of his society, and as well brings to his consciousness the latest of cyber threats. As the best proactive approach to problem is to know the problem and avoiding the problem itself, cyber security education exposes an individual to the knowledge of cyber threats, understanding its risks and causes and as such equipping him to respond proactively. It helps an individual to understand the effect of responding to the phishing emails, which has no purpose other than extracting the personal details for malicious purpose.

We live in a society where unsolicited bulk emails and SMS can easily be generated and sent to people on internet; hence an efficient cyber security education assists individuals in understanding the undermining risks of these acts, if response should be giving accordingly. Cyber security education helps an individual to understand the extent of information security on a giving communication system, and as well the associated risk that the individual should face by sending sensitive information through that medium.

It is the responsibility of government to formulate, supervise, and implement an effective cyber security policy which shall include punishment for the offenders; cyber security education brings to the knowledge of citizens this formulated strategies, and punishment associated with violating the cyber security laws, thereby educating the citizens on how to be a perfect law abiding citizens.

So many organizations require much personal information from individuals while having transactions with the organization, and might not have necessary infrastructures to keep the information safe; cyber security education helps an individual to understand and question organizations about the security of their data which might make the organization to beef up their security strategies in other to ensure the security of their customers` data.

Personal and mobile computing devices are becoming more common on daily basis; people no longer patronize public business centers as before, mobiles phones and Personal Digitals Assistances (PDAs) capacities are being increased to perform higher functions. Cyber security education enlightens an individual on how to make use of these devices, minimizing the effect of threats, and attacks on both personal basis and on public network.

People can now transfer files more efficiently than before using many available removable devices like: flash drives, floppy disks, scan disks, CD ROMs, and others; cyber security education helps an individual to understand that these removable devices could as well contain malicious codes which could cause harm to his or her personal information as well as computer itself.

Networks is the spice of modern technologies, it is now possible for people to communicate, share information and ideas more easily via networks, such as: Local Area Network (LAN), Metropolitan Area Network (MAN) or Wide Area Network (WAN); viruses, worms, and malicious codes could also be shared or transmitted through this means. Cyber security education helps an individual to understand this fact, and as such provide him with necessary measures to take, while connecting to this medium in other to avoid contacting these malicious infections.

IMPACT OF CYBERSECURITY EDUCATION ON ORGANISATION

The impact of cybersecurity education on organization is almost same as that on individual, but bearing in mind that organization manages both the corporate, and as well as personal data of individuals`; the need of cyber security education to organization becomes more important.

Many organizations like banks, insurance companies, and other corporate agencies usually capture some personal information from individuals that are their customers. This information constitutes one of the conditions that must be reached for the organization to establish a customary agreement with the individuals; cyber security education provides necessary information to organization on how hackers can manipulate the insiders to get sensitive information about their customers and as such advice them on how to avert the scourge.

Organizations are made up of various levels of management and employees which have variable functions and duties within the organization and handles customers data at deferent rates, cyber security education helps an organization to know the important of formulating policies which shall regulate and limit every department of the organization to its specific function by enabling the minimum privileges that could allow it perform its duties effectively.

Every nation has its cybersecurity regulations which an organization within it must be compliance; cybersecurity education impacts these regulations to the organization thereby making it not to violate the laws of the land.

The principle of defense in-depth has a lot to do with an organization managing a large volume of data, by separating different security layers and enforcing access controls and authentication mechanisms; cybersecurity education allows an organization to understand this principle and enforce it in other to ensure the maximum security of its customers` data. Many organizations do share some relationship with others relating to their various businesses and needs; cybersecurity education helps an organization to understand the security consciousness of their partners and as such know the level of partnership as regards to sharing their private information and data.

IMPACT OF CYBERSECURITY EDUCATION ON NATION

The evolution of these latest technologies embraced, and depends much on internet communication; in some countries all their gadgets have gone 'e' making life very simple and easier for its citizens. Countries now operates e-government whereby their classical information are being restricted to special people on internet which is not safe and other people could access this information at the comfort of the zones; Cyber security educations expose the various level of governments to the knowledge of the fact that their information is not safe, and advice them on how to manage it to a certain level to ensure that unwanted individuals could access it.

We live in a society whereby many nations are being challenged by another, histories has shown that many nations has being faced by cyber war leveraging one of their critical sector, rendering it unfunctionable; cyber security education helps a nation to understand this fact and educates its critical sectors on how to formulate an efficient cybersecurity policies which shall include cyber-incident response and recovery strategies to manage such an unforeseen occurrence.

Many nations play truants as regards to formulating an efficient cyber security policies; cybersecurity education helps a nation to understand the fact that collaborating with other nations where there is no efficient cyber security policy is risky and also makes them to redress their own in other to meet up with international standards.

The stage of having cyber security laws passed in some countries are still a dream; cyber security education helps a country to understand the danger they are facing by not passing a law that could prosecute any computer and network related crimes, and further expose them to the different ones which are in-force by other nations in other to enact their own.

CONCLUSION

The benefits of cybersecurity education to national security are numerous, as enumerated above, it ranges from the benefits to individuals through the benefits to the whole nation, cyber security education should be encouraged by every nation in other to equip their citizens about the latest strategies of cybercrimes and as well inform them on how to prevent the attack. Every nation should formulate a sector that should be saddled with the responsibility of sharing this cyber security education; this sector should also supervise the implementation of cyber security education in both primary and basic education curriculum. Cybercrime and crimes generally is better prevented from occurring than recovering after occurrence, cybersecurity education gives the proactive steps that helps in preventing a nation from being attacked by hackers.

Cyber security education should be encouraged by any nation that is willing to embrace the latest methods of communication as well as join the community of nations in moving to the cloud transactions system. Safety to individuals is safety to a nation, as safety to nations is safety to the world. The more you know about a disease and its cause, the more you avoid it. Every nation should take the issue of Cybersecurity on the front line of their security strategies in other to minimize its risk and encourage safe transaction experience.

ACKNOWLEDGMENTS

Our thanks to the management of Federal University of Technology for introducing the department of Cyber Security Science in the university, which has helped us in coming up with this write up.

REFERENCES

[1] (Macmillan Dictionary; Online version) Definition of National Security from Macmillan Dictionary (Online version) Macmillan Publishers Limited. Accessed July 17, 2013. http://www.macmillandictionary.com/dictionary/british/national-security

[2] Din(ThisdayLive, 2013) Definition of National Security from Senator Ike Eweremadu public lecture on "Policing and National Security in Nigeria: The Choices before Us" delivered at Nnamdi Azikiwe University, Awka, Nigeria. Available on ThisdayLive, Wednesday 17th July, 2013. Accessed 17th July 2013. Online at: www.thisdaylive.com/articles/policing-and-national-security-in-nigeria-the-choices-before-us/143666

[3] Sieber 2005. Sieber, Council of Europe Organized Crime Report 2004; ABA International Guide to Combating Cybercrime, 2002; Williams, Cybercrime, 2005, in Miller, Encyclopedia of Criminology.

[4] Gordon et al, 2006. On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20.

[5] (Chawki, 2005) Chawki, Cybercrime in France: An Overview, 2005, available at: http://www.crime-research.org/articles/cybercrime-in-france-overview

[6] Council of Europe Convention on Cybercrime. Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int

[7] ITU-GCA 2008. ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[8] *Walden, 2006.* Computer Crimes and Digital Investigations, 2006, Chapter 1.29

[9] ITU-CLR 2009. International Telecommunication Union: Cybercrime Legislation Resource: Understanding cybercrime; A Guide for developing Countries. ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector. Draft April, 2009.

[10] ITU-WTSA, 2008. ITU WTSA Resolution 52: Countering and combating spam. available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf

[11] WikiCS 2009. Online Wikipedia, computer security, accessed on July, 2013. Available at http://en.wikipedia.org/wiki/Cyber_security

[12] Multi-state Information Sharing and Analysis Center (MS-ISAC) 2010. Multi-state Information Sharing and Analysis Center (MS-ISAC), A Division of Center for Internet Security: 2010 National Cyber Security Awareness Month, After-Action Report, page 2.