A PUBLICATION OF INTERNATIONAL ASSOCIATION FOR THE PROMOTION OF ASIA-AFRICA RESEARCH IN COLLABORATION WITH MEDICAPS UNIVERSITY, INDIA

Asia-Africa Journal of Education Research
A Publication of International Association for the Promotion of Asia-Africa Research
Vol. 2, 2022
DOI: 10.5281/**zenodo**.6370137
ISSN: 2814-1409
Copyright: Author(s) retain the copyright of this article
https://journals.iapaar.com/index.php/aajer

CYBER SECURITY: TRENDS AND CHALLENGES TOWARD EDUCATIONAL DEVELOPMENT IN 21ST CENTURY

Nseabasi, P. Essien Ph.D
Department of Industrial Technology Education,
Faculty of Education,
University of Uyo,
Akwa Ibom State
nseabasiessien@uniuyo.edu.ng

and

Ekaiko, Ukeme Aniefiok
Department of Industrial Technology Education,
Faculty of Education,
University of Uyo,
Akwa Ibom State
u.ekaiko1@gmail.com

Abstract

Cyber Security is a combination of processes, technologies and practices. The objective of Cyber Security is to protect programs, application, networks, computers and data from attack. In a computing context, security includes both cyber security and physical security. The attacker damage or theft software or information. Cyber security includes controlling physical access of the hardware, application networks and protecting against harm that may come via networks. Cyber security plays a vital role in the discipline of information security. Preventing the information has become one of the major challenges in the current scenario. Cybercrime is one of the significant factors in cyber security, it increased daily. Numerous educational bodies and other sectors are taking many measures in order to secure these cybercrimes. Handling cyber security is still a very huge concern. This research paper mainly focuses on the challenges faced by cyber security on the latest technologies towards educational development in 21st Century. It also focuses on latest about the trends changing the face of cyber security towards educational development in 21st Century.

Keywords: Cyber Security, Cyber Crime, Parameters of Cyber Security and Security Attacks.

Introduction

Data communication is playing a major role in today's human life through sending and receiving any form of data like text, image, video or audio files just by clicking the button but that person don't know whether that message transmitted or sent to the other person safely without any leakage of information. In today's technical environment many recent technologies are belonging to the fast growth of internet technology. But according to these emerging technologies are unable to prevent the private information in a very effective way and hence, in this 21st century cyber crimes are increasing daily. Recently, more than 60 percent of total commercial transactions are done through online, so this field required a high quality of security for transparent and best transactions.

Pusey& William (2012) pointed out that cyber security has become a latest issue in the IT sector. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like educational sector etc. The latest technologies like cloud computing, green computing, mobile computing, E-commerce, net banking are required high level of information security. According to Parashu (2015), he sees cyber crime as a term for any illegal activity that uses a computer as its primary means of commission and theft.

The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime as pointed out by Kartikey & Sanjay (2014), defined as crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent.

Concepts of Cyber Security

Ravi (2003) asserts that cyber security is the protection of systems, networks and data in cyberspace and is essential even as more people get connected to the internet across the world. The international Telecommunications Union (ITU) defines Cyber security as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

The ITU also notes that the three broad security objectives are ensuring Availability; Integrity (which may include authenticity and non-repudiation), and confidentially. While these are the bedrock of a secure network, achieving these three objectives is no mean feat as it requires the integration of various functions such as robust systems engineering and configuration management; effective cyber security or information assurance policy and comprehensive training of personnel. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment - the internet (Steffani, 2006). Cyber Security can also be described as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access (Thilla, 2012).

Cyber Security:

Shikha (2015) defined cyber security as a term of security which is implicated through diversified disciplines, most of them focusing on technical or psychological problems such as computer science, criminology, economics, engineering, information systems, management, medicare, neurophysiology, psychology, sociology, etc. It affords the people with discussions about behaviours and motivations, benefits and consequences about cyber crime and security. Cyber security will be used to represent the security issues of information systems: Cyber security is one of the information system management by individuals or organizations to direct end-users security behaviours, on the basis of personal perceived behaviours toward potential security breach in work and non-work environment. Farhad &Thurai (2016) asserted that the extant study of cyber security explores three main streams that if properly utilized or considered can guard against some cyber trends and challenges towards educational development in 21st century. Such as; individual behaviours toward information security in non-work setting, employee behaviours toward information security in work setting, and organization information system security policy (ISSP) compliance and the related issues.

Functions of a Cyber Security Center:

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

i. Serve stakeholders as a national center of excellence and expertise for cyber and telecommunications security issues.

ii. Focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the Nation;

iii. Pursue whole-of-nation operational integration by broadening and deepening engagement with its partners through information sharing to manage threats, vulnerabilities, and incidents.

iv. Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact.

v. Maintain a sustained readiness to respond immediately and effectively to all cyber and telecommunications incidents of national security.

vi. Protect the privacy and constitutional rights of the citizens in the conduct of its mission.

Concepts of Cyber Risk

Cyber risk can be defined as the risk connected to activity online, internet trading, electronic systems and technological networks, as well as storage of personal data. According to Deloitte Advisory Cyber Risk Services (2013), the fundamental things that organizations undertake in order to drive performance and execute on their business strategies happen to also be the things that actually create cyber risk. This includes globalization, mergers and acquisitions, extension of third-party networks and relationships, outsourcing, adoption of new technologies, movement to the cloud, or mobility.

Cyber risk is an issue that exists at the intersection of business risk, regulation, and technology. Events covered by this more comprehensive definition can be categorized in multiple ways. One is intent. Events may be the result of deliberately malicious acts, such as a hacker carrying out an attack with the aim of compromising sensitive information, but they may also be unintentional, such as user error that makes a system temporarily unavailable (www.reuters.com). Risk events may come from sources outside the organization, such as cybercriminals or supply chain partners, or sources inside the organization such as employees or contractors. Combining these two dimensions leads to a practical framework for inventorying and categorizing cyber risks into:

Internal Malicious: Deliberate acts of sabotage, theft or other malfeasance committed by employees and other insiders. For example, a disgruntled employee deleting key information before they leave the organization.

Internal Unintentional: Acts leading to damage or loss stemming from human error committed by employees and other insiders. For example, in 2013, NASDAQ experienced internal technology issues that caused backup system to fail.

External Malicious: the most publicized cyber risk; pre-meditated attacks from outside parties, including criminal syndicates, hacktivists and nation states. Examples include network infiltration and extraction of intellectual property, and denial-of-service (DoS) attacks that cause system availability issues, business interruptions, or interfere with the proper performance of connection devices such as medical devices or industrial systems.

External Unintentional: Similar to the internal intentional, these cause loss or damage to business, but are not deliberate. For example, a third party partner experiencing technical issues can impact system availability, as can natural disasters

Areas in Cyber Securities Related To Educational Sector

The major areas which are included in cyber securities in educational sector as stated by Wright, Dawson, Maurice & Omar (2012) are as follows:

Application Security

Any software the user can use to run their business needs to be protected, whether the IT staff builds it or whether the user can buy it. Any application may contain holes, or vulnerabilities, those attackers can use to infiltrate user's application. Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance.

Security measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

Information Security

Information security is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Information security programs are built around the core objectives like maintaining the confidentiality, integrity and availability of IT systems and business data. These objectives ensure that sensitive information is only disclosed to authorized parties (confidentiality), prevent unauthorized modification of data (integrity) and guarantee the data can be accessed by authorized parties when requested (availability).

Email Security

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

Mobile Device security

Cyber criminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, the users need to control which devices can access their network. The user will also need to configure their connections to keep network traffic private.

Web Security

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

Wireless Security

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, user need products specifically designed to protect a wireless network.

Cyber Security Parameters

Nakama & Paullet (2019) highlighted some cyber security parameters in the journal: *The urgency for cyber security education.* They stated that Cyber security has some of the parameters which are as follows. Figure 1 depicts about the various kinds of cyber security parameters. Such as;

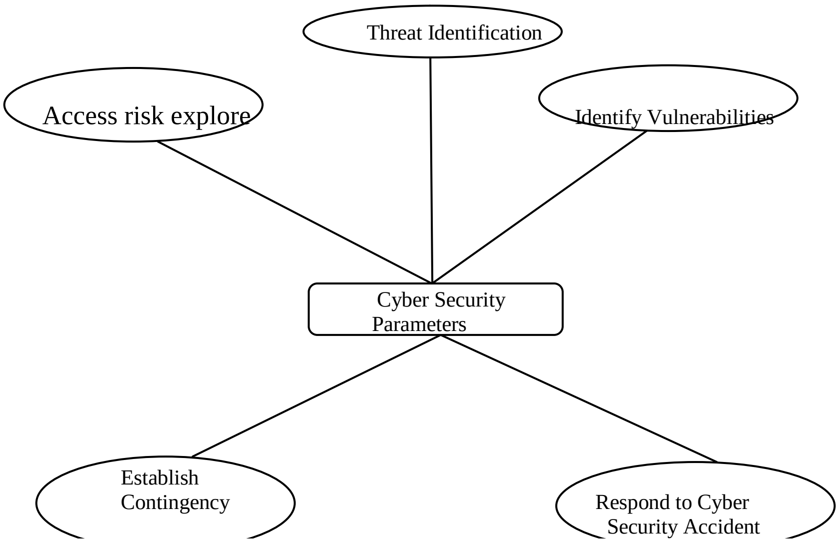

Fig. 1 Cyber Security Parameters

Identify threats

In computer security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.

A threat can be either a negative "intentional" event (i.e. hacking: an individual cracker or a criminal organization) or an "accidental" negative event (e.g. the possibility of a computer malfunctioning, or the possibility of a natural disaster event such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.

This is differentiated from a threat actor who is an individual or group that can perform the threat action, such as exploiting a vulnerability to actualize a negative impact.

Identify Vulnerabilities

This activity is focused on identifying vulnerabilities that could be exploited by the threats that you have identified. The existence of vulnerability is a major contributing factor for calculating the probability of risk. If an asset has a vulnerability that can be exploited by a threat, then the risk to that asset is much higher when compared to an asset that does not have the same vulnerability. If a system has weak passwords, a hacker who is able to find and leverage a “weak password” in an information system has a greater chance of achieving unauthorized access. Therefore, we can see here that vulnerability increases the probability of a threat source achieving its threat action.

The objective of this activity is to determine all potential vulnerabilities to the asset that could be leveraged by a threat source. The outcome of this activity is typically captured in the form of a vulnerability listing. There are actually two possible approaches to take here. Either you make a comprehensive vulnerability listing of all possible vulnerabilities that you can think of or you can focus only on the vulnerabilities that have already been identified within the organization.

Access Risk Explore

Broadly speaking, a risk assessment is the combined effort of:

a. Identifying and analyzing potential (future) events that may negatively impact individuals, assets, and/or the environment (i.e. hazard analysis); and

b. Making judgments "on the tolerability of the risk on the basis of a risk analysis" while considering influencing factors (i.e. risk evaluation).

Risk assessment determines possible mishaps, their likelihood and consequences and the tolerances for such events. The results of this process may be expressed in a quantitative or qualitative fashion. Risk assessment is an inherent part of a broader risk management strategy to help reduce any potential risk-related consequences.

Establish Contingency Plan

A contingency plan is a plan devised for an outcome other than in the usual (expected) plan.

It is often used for risk management for an exceptional risk that, though unlikely, would have catastrophic consequences. Contingency plans are often devised by governments or businesses. For example, suppose many employees of a company are traveling together on an aircraft which crashes, killing all aboard. The company could be severely strained or even ruined by such a loss. Accordingly, many companies have procedures to follow in the event of such a disaster. The plan may also include standing policies to mitigate a disaster's potential impact, such as requiring employees to travel separately or limiting the number of employees on any one aircraft.

Respond to Cyber Security Accident

Incident response planning should be part of educational organization’s cyber security regime, alongside risk management and cyber security breach detection. An incident response plan can help safeguard your organization especially educational sectors and protect it against the impact of cyber crime.

It's important to plan your cyber security incident response before you actually detect any intrusions. As part of this process, consider ways in which you will handle cyber security and your readiness to:

a. Prepare for an incident
b. Deal with a cyber breach or intrusion
c. Follow up a cyber security incident

It's best to decide in advance how you will manage these different aspects of your response.

Educational Related Security Attacks and Types

According to Ghafir (2014), he sees Security Attack as any action that compromises the security of information owned by an organization using any process that designed to detect. There are several types of attacks, but most common security attacks related to educational sector are described below:

Denial of Service Attacks

These attacks are mainly used to unavailable some resources like a web server to users. These attacks are very common today. They used overload to resource with illegitimate requests for service. The resource cannot process the flood of requests

Brute Force Attacks

These attacks try to kick down the front door. It’s a trial-and-error attempt to guess a system’s password. One in four network attacks is a brute-force attempt. This attack used automated software to guess hundreds or thousands of password

Browser Attacks

These attacks target end users who are browsing the internet. The attacks may them to unwittingly download malware. These attacks used fake software update or application. Websites are also force to download malwares. The best ways to avoid browser-based network attacks is to regularly update web browsers.

Shellshock Attacks

These attacks are refers to vulnerabilities found in Bash, a common command-line shell for Linux and UNIX systems. Since many systems are never updated, the vulnerabilities are still present across the Web. The problem is so widespread that Shellshock is the target of all networks.

SSL Attack

These attacks are intercept data that is sent over an encrypted connection. These attacks successfully access to the unencrypted information. These attacks are also very common today.

Backdoor Attacks

These attacks are used to bypasses normal authentication to allow remote access. These attacks are added in software by design. They are added in the Programs or created by altering an existing program. Backdoors is less common types.

Botnet attacks

These attacks are hijackers. They are computers that are controlled remotely by one or more malicious actors. Attackers use botnets for malicious activity, or rent the botnet to perform malicious activity for others. Millions of computers can be caught in a botnet’s snare.

Strategies to Strengthen Cyber Security

Based on the World Economic Forum (2012) research findings, most Nigerian organizations are ill-equipped to respond to information security threats. Although there are different initiatives (regulators, government and private organizations) in place set out to address information security issues in Nigeria, these initiatives cannot adequately address the current information security issues. Public and private organizations need to rethink their whole approach to information security and establish security practices needed to protect critical IT infrastructure. They also need to train and grow security experts needed to secure this infrastructure. Most organizations now recognize that it is imperative that local organizations take action before the situation worsens and the cost of inaction becomes even greater (World Economic Forum, 2012). Lamorde (2015) maintained that just as it is with the European Union, North America and several countries in Asia have come up with National Strategy on Cyber security. The Nigerian National Cyber security framework should consider internet security as vital to a vibrant digital society. It should set out action plans to improve cyber security readiness and provide response and management of breaches for all internet users.

Lamorde (2015) suggested that the strategy should include the establishment of a well-functioning network of Computer Emergency Response Team at the national level. The organization of cyber incidents simulations, putting in places a well-defined policy on Critical Information Infrastructure Protection (CIIP) with the aim of strengthening the security of ICT Infrastructure. He advised that in order to ensure a safer internet for our kids and young persons, the framework should create a strategy that will provide a safer and more secured cyber space for our young ones. Juwah (2015) assert that countries need to step up; work together to build and provide information security services that enables Nigeria to address these challenges. Nigerians need to leverage their local presence and understanding of the environment to provide a clear indication of the security problems on the ground. This local presence combined with partnerships with regional and global players will provide globally tested solutions and approaches to address identified security problems.

Solutions to cybercrime

Education: Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

Establishment of Programs and IT Forums for Nigerian Youths: Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT in Nigeria at the number of cryptographic methods have been developed and some of them are still not cracked.

Cyber Ethics and Cyber legislation Laws: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber-crimes will reduce. Security software like anti viruses and anti-spy wares should be installed on all computers, in order to remain secure from cyber-crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious programs.

Conclusion

Cyber security is a vast issue that is becoming more essential because the world is becoming extremely interconnected, with networks being used to carry out critical transactions. Security is a very complicated and vital important topic of today's information technology. Everyone has a different idea regarding security policies and levels of risks. The key for building a secure network is to define what security need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Hence security plays a vital role in information security. Cyber crime continues to deviate down different paths with each novel Year that passes and so does the security of the information. The newest and disturbing technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no proper solution for cyber crimes but using recent techniques to minimize the cyber crime in cyber space.

References

Annasingh, F. and Veli, T. (2016). *An investigation into risks awareness and e-safety needs of children on the internet, Interactive Technology and Smart Education*, vol. 13, no. 2, pp. 147-165.

Akpan, E. (2020), *A Critical Analysis Of cyber Security and Resilience in Nigeria.* World Atlas Journal of Library and Information Science. Vol. 5 No.1. New York City

Bhavani, T. S. & Latifur, K. (2008). Data Mining for Security Applications. International Conference on Embedded and Ubiquitous Computing

Farhad, A., Sanjay, P. (2015). Usage of data Mining Techniques for Combating Cyber Security: International Journal of Engineering and Computer Science. Vol. 6, Page No. 20011-20016

Ghafir & Prenosil, V. (2014) "*Advanced Persistent Threat Attack Detection: An Overview*", International Journal Of Advances In Computer Networks And Its Security, Vol. 4, Issue. 4, pp. 50–54,.

Kartikey, A. & Sanjay, K. D. (2014). Network Security: Attacks and Defense in International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1, Issue 3.

Nakama, D. & Paullet, K. (2019). *The urgency for cyber security education: The impact of early college innovation in hawaii rural communities*, Information System Education Journal, vol. 16, no. 4, pp. 41-52.

Pusey, P., & William, A. S. (2012). *Cyber ethics, cyber safety, and cyber security:* Per service teacher knowledge, preparedness, and the need for teacher education to make a difference, Journal of Digital Learning in Teacher Education, pp. 82-88.

Parashu, R. P., (2015). Cyber Security Issues and Challenges, A Review: A Recent study Over Cyber Security and its Elements, Lakshmi Narain College of Technology, Bhopal, M.P., India

Shikha, A. & Jitendra, A., (2015). Survey on Anomaly Detection using Data Mining Techniques" in 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems Available online at www.sciencedirect.comProcedia Computer Science 60, pp 708 – 713

Wright, J., Dawson, M., Maurice & Omar, Marwan. (2012). "*Cyber Security and Mobile Threats: The Need for Antivirus Applications for Smart Phones*", Journal of Information Systems Technology and Planning. Vol. 5. pp. 40–60.