academicresearchJournals

Vol. 8(2), pp. 22-26, March 2020
DOI: 10.14662/IJALIS2020.035

ISSN: 2360-7858
http://www.academicresearchjournals.org/IJALIS/Index.htm

International Journal of Academic Library and Information Science

Full Length Research

Cybersecurity Threats and Its Emerging Trends on Academic Libraries

Ibrahim, Hassana Ozavize and Umar, Fatimah Abedo

College Library, Federal College of Education, Okene, Kogi state.
Email: hassanaozavize@gmail.com, Tel: 08068450710

Accepted 29 February 2020

The paper examined cybersecurity threats and its emerging trends on academic libraries. The paper focused on cybersecurity and kinds of cyber security threats. The paper employed an explanatory method. The study concluded that the issue of cyber security in university libraries is an issue that requires serious managerial and strategic attention. The paper added that the latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging academic libraries with not only how they secure their information resources, but how they require new platforms and intelligence to do so. However, there is no absolute solution to cyber security threats in the library, but a number of strategies can be employed to help reduce its increasing nature. The paper also recommended that academic libraries should secure their network information; improve awareness and competence in information security and sharing of best practices through the development of a culture of cybersecurity at all levels in the library; implement an evaluation/certification programme for cyber security product and systems and among others.

Keywords: cybersecurity threats, university libraries, academic libraries, network information

Cite This Article As: IBRAHIM, HO., UMAR, FA (2020). Cybersecurity Threats and Its Emerging Trends on Academic Libraries. Inter. J. Acad. Lib. Info. Sci. 8(2): 22-26

INTRODUCTION

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. Security remains near the top of the list of strategic issues facing higher education institutions. Given the increasing volume of information that needs to be protected, the expanding body of rules, regulations, and laws governing information security and privacy, and the current economic downturn, which makes it even harder for an institution to obtain the funding necessary to keep up with requirements, this is not at all surprising. Security is not strictly a technology matter; indeed, it is a foundational element for almost all academic libraries. Responsibility for security needs to extend beyond information technology to every functional office in the institution and to the highest level of management.

Different libraries have adopted varying security measures for their collections' safety. McComb (2004) writes that physical (non-electronic) security, electronic security and security policies/procedures are substantial methods for securing information resources of all kinds of libraries. Physical security includes architectural considerations, the use of personnel, and security hardware to prevent crimes against library collections. Electronic security system refers to the use of equipment which typically provide alarm notification to the appropriate authority on entry control and site surveillance. Major elements of the electronic security

system include burglary protection, collection security (hidden on materials), access control (systems that directly “read” unique personal characteristics such as voice quality, hand geometry, identity cards, etc.), and video surveillance, particularly the CCTV system. Sensors (detectors) to detect an intrusion and alarms (to notify appropriate authorities) are the facilities that make this type of security electronic. On the other hand, security policies and procedures include all created and implemented security policies, procedures, and plans for the library. These should, at least, include entry and exit procedures, room registration procedures, personal belonging restrictions, special collections use policies, and entry key management procedures (McComb, 2004).

Cybersecurity is concerned with making cyberspace safe from threats, namely cyber-threats. Typical cybersecurity issues, according to Udotai (2002) in Odumesi (2006) include: confidentiality of information; and integrity of systems and survivability of networks (CIS). Major objective of cybersecurity includes: protection of system/networks against unauthorised access and data alteration from within; and defense against intrusion from without. As commonly used, cybersecurity, according to Ajie (2019), refers to three things: a set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and software devices, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to national security; the degree of protection resulting from the application of these activities and measures and the associate field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality.

Kinds of cyber threats

The following are forms of Cyber threats as identified by Ajie (2019):

Hardware Security Threats: Hardware, form as a physical component in an information system is also prone to security attacks. Previous study results (Ke, 1997; Lin and Huang, 1999; and Shen, 1999) revealed several factors that jeopardise hardware security including: natural disasters such as earthquakes, fires, floods and thunder strokes; changes in temperature or humidity; accidents, such as stealing and vandalism; malicious intrusion and destruction; defects of the hardware itself, such as bugs or errors generated from routers or firewalls; faults in the manufacture of the equipment; air-conditioning failure; loss of essential services such as telecommunications or power. Other hardware security threats include electromagnetic interference, failure of communication equipment and services, hardware equipment failure, installation of unauthorised hardware, maintenance errors, physical sabotage or intentional destruction of computing equipment, theft, physical sabotage and vandalism of ICT hardware equipment. Farahmand (2003) indicated that hardware attacks can be mounted against hardware for the purpose of using the hardware as a means of denying use of the system. These may include a physical attack against the equipment, a bug implanted within the hardware or an attack against the supporting utilities. Computer hardware infected with malware (i.e. computer viruses, worms and Trojan horses) may suffer some sort of damage such as making it impossible to boot the computer, repeated error messages, hardware malfunctions and lowered the computing speed.

Software Security Threats: In terms of jeopardising software security, the threats can be divided into operating systems and related applications. Security threats associate with operating systems might include the security loopholes due to improper design and improper management. Whereas, software security threats related with applications include stealing or copying software from the Internet which might contain viruses (Shen, 1999). Computer software infected with malware (i.e. computer viruses, worms and Trojan horses) may suffer some sort of damage such as periodically automatic reboots, program crashes or malfunctions, repeated error messages and poorer system performance or unusual behavior. Other software security threats include corruption by system, system failure, maintenance errors, cyber-terrorism, software piracy, unauthorised access, unauthorised changes to software settings, adware, spyware, hacking, password sniffing, weak passwords and abuse of computer access control. There are several software security threats that could jeopardise software security such as follows: abuse of computer access control refers to employees or patrons abusing their access controls rights and privileges for personal reasons or to obtain more data than needed for their jobs; adware and spyware is a type of malware that can be installed on computers to collect information about users without their knowledge. Specifically, adware is used as a marketing tool to monitor people's behaviour on the Internet, to determine which products they are interested in. Whereas, the functions of spyware extend well beyond simple monitoring. Spyware programs can change computer settings, resulting in slow connection speeds and loss of Internet connection or functionality of other programs; corruption by system, system errors, or failure of system software. According to Laprie (1992) “a system failure occurs when the delivered service no longer complies with the specifications". Whereas, an error is defined by

Laprie (1992) as that part of the system which is liable to lead to subsequent failure, and an error affecting the service is an indication that a failure occurs or has occurred. If the system comprises of multiple components, errors can lead to a component failure. As various components in the system interact, failure of one component might introduce one or more faults in another. Hacking refers to unauthorised attempts to bypass the security mechanisms of an information system or network either skilled or unskilled persons. Internet threats such as malicious code, Trojans and spyware could make desktop vulnerable to leakage of important corporate information (Gawde, 2004). A password is also vulnerable to sniffing or stealing every time it sent across a network such as when users are using remote access to access computers, printers, databases, emails or Internet banking. The use of pirated or unauthorised software on the library network is illegal and places the library in danger of legal action by the software supplier. Thus, ensuring that the software on library computer systems is fully licensed is a responsibility of the IT personnel as f libraries are found to be in noncompliance, the consequences can be quite expensive. Unauthorised changes to software settings or to program code can be used to commit fraud, destroy data or compromise the integrity of a computer system. This would involve a manipulation of settings in the browser such as to delete history files, change security settings or enable private browsing. Use of library Internet for illegal or illicit communications or activities such (e.g. porn surfing, e-mail harassment or porn surfing).

Network Security Threats: Williams (2001) listed the most common network security threats in small libraries such as; a) Cracking of passwords; **d**amage to equipment or data due to lightning strike, surges or inadequate power; **i**nternet based attacks of internal network resources; **l**ocal patron tampering workstation desktop and systems that the intruder has found to be vulnerable (Eisenberg and Lawthers, 2005)**.** Transmission errors may occur due to the failure of any of the network components that are used for the transmission of data. These errors can destroy the integrity and reliability of data and can lead to a loss of availability; **w**ebsite defacement is an attack usually initiate by a system cracker who breaks into a web server and changes the visual appearance of the website. Penetration and hacking of web sites is increasing due to the growth of virtual private networks and online business.

Data Security Threats: Data security is the practice of protecting and ensuring privacy of personal or corporate data resides in databases, network servers or personal computers from corruption and unauthorised access. The threats include: destruction of information and other resources, corruption or modification of information, theft, removal or loss of information and other resources, disclosure of information and interruption of services. Also, there are several other threats that could jeopardise data security such as follows: data diddling or changing of data before or during input into a computer system; data loss due to wrong procedures of updating, storage or backup; data manipulation; delay in updating or dissemination; destruction due to natural disaster; exposure of patrons sensitive data through web attack; impersonation or social engineering; loss of patron data or privacy ideas; malware and Malicious code (e.g. virus, worm, Trojan horse, logic/time bombs and trapdoor); masquerading of user identity; Password attacks, sniffing, stealing, phishing or pharming; theft of proprietary data; unauthorised access; unauthorised data copying; unauthorised transfer of data; and Unauthorised, accidental disclosure, modifications or alteration of data (Ajie, 2019).

Physical Facilities and Environmental Threats: The most common problem of physical threats that must be factored into a security program includes natural disaster and theft. It has been reported that the relationship between physical threats and virtual threats is most apparent as both physical infrastructure and systems are needed to provide an access point to the virtual world (Lindstrom, 2003). Tittel (2003) listed the most common types of physical threats including: fire and smoke; water (rising or falling); earth movement (earthquakes, landslides or volcanoes); storms (wind, lightning, rain, snow, sleet or ice); sabotage or vandalism; explosion or destruction; building collapse; toxic materials; utility loss (power, heating, cooling, air or water); equipment failure; and personnel loss (strikes, illness, access or transport). Also, computing equipment, physical infrastructure assets and data can be destroyed due to fire, floods, electricity spikes and power outages. However, chemical, radiological and biological hazards can also cause damage to electronic equipment both from intentional attack or accidental discharge in an information system environment (Vacca, 2009). Intrusion or authorised access into library building is seen as another threatening threat which can lead to theft of valuable materials.

Human Related Threats: Several studies revealed that human errors are the most highly ranked security threats (Loch, Carr and Warkentin,1992; Whitman, 2004; Im and Baskerville, 2005). Human errors include the following: poor passwords selection, piggybacking, shoulder surfing, dumpster diving, installing unauthorised hardware and software, access by unauthorised users and social engineering, lack of discipline or knowledge among library staff and patrons (Pipkin, 2000 and Conklin, 2005). Human errors including data entry errors or carelessness, though often not considered as threats

but they are highly likely to occur. Lindstrom (2003) revealed that erroneous actions by employees or users can threaten the integrity, availability, confidentiality and reliability of data. Examples include: Incorrect set-up of security features could result in loss of confidentiality, integrity and availability of data; switching off computers when an error is displayed instead of correctly closing all current applications; deletion of files; inadequate back-ups; and processing of incorrect versions of data.

Mechanisms to combat cyber threats in academic libraries

The measures taken to protect the library systems, buildings and related supporting infrastructures or resources against cyber security threats have witnessed massive consideration. Davis (n.d) highlighted seven safety actions that academic libraries can adopt and they are:-

1. Run Anti-virus Software: - To avoid computer problems caused by viruses, its necessary to install and run anti-virus programmes periodically and to always update it. Antivirus software removes viruses, quarantines and repairs infected files and can help prevent future viruses.
2. Install software updates: Updates sometime called *patches* fix problems with operating systems and software programmes.
3. Prevent Identity Theft: Financial account numbers, Social security numbers and details on drivers license or personal identity information should not be given out. Another thing to look out for is phishing scams which is a form of fraud that uses email messages that appear to be from a reputable business in attempt to gain personal or account information.
4. Turn on Personal Firewalls: Firewalls act as protective barriers between computers and the internet. If computers have built in fire walls, hackers who search the internet by sending out pings (calls) to random computers and wait for response will wait in vain. Firewalls prevent your computer from responding to these calls.
5. Avoid Spyware/ Adware: Spyware and Adware should be avoided because they take up memory ad can slow down your computer or cause other problems.
6. Protect Passwords: Passwords should not be shared and new passwords should be difficult to guess by avoiding dictionary words, mixing letters, numbers and punctuation. Passwords should be a mixture of upper and lower case letters, minimum of 8 characters and mnemonics to help remember a difficult password.
7. Back up important files: To reduce the risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.

CONCLUSION

Cyber security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Thus, the issue of cyber security in university libraries is an issue that requires serious managerial and strategic attention. Cyber security should not be allowed to gain expression in academic libraries due to their financial and social consequences. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging academic libraries with not only how they secure their information resources, but how they require new platforms and intelligence to do so. However, there is no absolute solution to cyber security threats in the library, but a number of strategies can be employed to help reduce its increasing nature.

RECOMMENDATIONS

The paper suggests the following as mechanisms to combat cybersecurity threats in academic libraries:

1. Safeguarding the privacy rights of individuals when using electronic communications
2. Academic libraries should secure their network information.
3. Improving awareness and competence in information security and sharing of best practices through the development of a culture of Cybersecurity at all levels in the
4. Implement an evaluation/certification programme for cyber security product and systems.
5. Institutional framework should be formed that will be responsible for the monitoring of the information security situation, dissemination of advisories on latest information security alerts and management of information security risks including the reporting of information security breaches and incidents.

REFERENCES

Adewole .S.K & Olayemi.R (2011). An inquiry into the awareness level of cyber security policy and measures in Nigeria. *International Journal of Science and*

Advanced Technology. 1(1).

Ajie, I. (2019). A Review of Trends and Issues of Cybersecurity in Academic Libraries. *Library Philosophy and Practice (ejournal)*.https://digitalcommons.unl.edu/libphilprac/2523

Davis (n.d), Cyber –Safety Basics.

Eisenberg, J. and Lawthers, C. (2005).Library computer and network security. *Info people.* From http://www.infopeople.org/resources/security/.

Farahmand, F., Navathe, S. B., Sharp, G. P., and Enslow, P. H. (2003). Managing Vulnerabilities Of information systems to security incidents, Pittsburgh.

Gawde, V. (2004). Information Systems Misuse - Threats & Countermeasures. *Info sec writers.*

From http://infosecwriters.com/text_resources/pdf/information_systems_misuse.pdf.

Im, G. P. and Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *SIGMIS Database*. 36(4): 68-79.

Lindstrom, P. (2003). Let's Get Physical: The Emergence Of The Physical Threat. *A Spire Research Report*. http://www.netbotz.com/library/Physical_Threat_Security.pdf.

Loch, K.D., Carr, H.H. and Warkentin, M.E., (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*. 16 (2): 173-186.

McComb, M. (2004). Library security. San Francisco: RLS Inc.

Odumesi, J.O. (2006). Combating the menace of cybercrime: The Nigerian Approach (Project), Department of Sociology, University of Abuja, Nigeria p.45.

Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*. Prentice Hall PTR: Upper Saddle River, New Jersey.

Shen, W.Z. (1999). Attack and protection with Hacker. *Communication of Information Security*. 5(3):86–96.

Tittel, E., Chapple, M., and Stewart, J. M. (2003). *CISSP: Certified Information Systems Security Professional study guide.* 3rd. ed. Sybex: Wiley Publishing.

Vacca, J.R. (2009). *Computer and information security handbook*. Burlington: Morgan Kaufmann Publication. p.632.

Williams, R. L. (2001). Computer and network security in small libraries: A guide for planning. *Texas State Library & Archives Commission*. From http://www.tsl.state.tx.us/ld/pubs/compsecurity/.