Global Review of Library and Information Science (GRELIS)
Vol. 19, No. 2, 2023
ISSN: 3428-0009

THE HUMAN PERSPECTIVE OF LIBRARY INFORMATION MANAGEMENT AND SECURITY SYSTEM

By

OKEREKE, CHIDIOGO ADAOBI

Abstract
The paper focuses on human perspective as a threat to information management and security in a university library. The paper shows that majority of the university recognized that their staff, who are mostly thought of the weakest links in information management and security, also can be great assets in the effect to reduce risk associated with data management and security. The paper also highlights the emergence of the dangerous online activities, Smartphone's, it's capabilities, its wide adaptabilities and its threat to Informationmanagement and security as used by internet fraudsters to commit such reprehensible crimes as cyber cracking, extortion etc.

Keywords: Human Aspects, Management and Security Awareness, Smartphone, Malware, Information.

Introduction

An "Information System" is a complete apparatus for handling all aspects of information within a university environment. It includes everything from the completely human-orientated aspects of information to the technologically oriented aspects. The major components of an information system are the Data Processing systems which provide much of the information that is needed throughout a university library system. The human factor has a tremendous impact on the success and failure of our efforts to secure and defend our library information management and security.

Information security is complex and ever changing. Information management and security is protecting information from unauthorized access, use, disclosure, modification, distraction, or recording either in physical or electronic format. Human perspective is an approach to psychology that emphasizes empathy and stresses the good in human behavior. A humanistic approach to helping someone build self- esteem would involve encourage a person to focus on their strengths rather than their faults. Human perspective in web browsing habit is

ISSN: 3428-0009

dangerous as it can lure the surfer into malicious intention to hack information on the web. Information is an essential resource for the development of any nation. It is the hub of the library, government, communication, science and technology etc.

This day it is generally more applied to some form of computer system security because of its wider adaptability for information management. Globally, cybercrime as human perspective is now a common phenomenon. Hardly any day without report of data breach or other cyber related scam. Information security fraudsters have considerable resources and expertise to operate at any level. In developing countries of Africa like Nigeria, information security is under serious threat. Cyber criminals have organize networks that hack into university libraries, government or individual security information using more sophisticated mobile Smartphone's, to cause significant damage to their becoming a dangerous communication tool highly associated with some heinous criminal web activities such as cyber extortion, cracking, Phishing, terrorism, theft, span, kidnapping etc. The difference between nations is their difference in information resource and use. Technology today is helping to fast track needed information for education and development.

In Nigerian university libraries, the Smartphone as a human perspective is widely used as information resource tool. Many students, lectures and researches use the Smartphone to access, store and share information from the university e-library, academic search complete and the Hein online academic core law library online databases. Many of the students also use the gadget to create audio recording of their lecture note and sent created files to their desktop via e-mail. The Smartphone is also used by many in the university library community as personal organizers, access bank account, communicate with friends on social media, send short messages (SMS), download, take photographs etc.

ISSN: 3428-0009

In any university, information is essential for effective teaching, learning and research. Consequently, the use of a Smartphone in accessing library resource is to enhance quick access and use of the information. As a result, any attack on the library online information resource is catalyst to development.

Threat on information security

Despite the many good things about the human perspective online activities, they constitute a potential threat to management and information security globally, for instance, the alert notification software constitute annoying nuisance and distraction that can condition a user to always pull out the phone at every notification to perceive the message.

Togo (2015) posits that the Smartphone as a repository of personal information creates large security risk because if stolen, the thief did have accesses to the owner's potential data. Even where the phone is secured with a password, a remote wipe can destroy all the data on the phones hard drive system. The European Union agency for Network and information security, ENISA (2015) also posit that a thief can use the Smartphone infected with malware to intercept SMS authentication codes to attack online banking application. The strategy is for an attacker to submit an online application impersonating a real banker. If a user download and use the application, the criminal then mount a middle- main attack using the transaction details. Yet a criminal can deploy a rogue network access point and Smartphone users connect to it. The criminal afterwards intercept the users communication process to execute further attack such has phishing. Rogue internet gateway names can be configured on the Smartphone by a malicious SMS is used to change the default access point used by the phone.

The hardware required to set up such a base station has become relatively inexpensive (ENISA 2015).With the Smartphone, it is also possible for an attacker to hack sensitive files

ISSN: 3428-0009

placed on university library wed server by stepping out of the root directory using the dot slash (../)to execute some commands. All the attacker needs is a web browser and some knowledge on where to blindly find any default files and directories on the system to perform the malignant act.

A major concern inside information and management security is the threat of social engineering attacks. Assailants utilizing social engineering try to increase sensitive information focusing on human vulnerabilities that are weaknesses in an organization's management and security as a result of the attributes and behaviours of people .Information Management and security awareness can be defined as the level of comprehension that users have about the importance of information management and security best practices. Information management and security awareness becomes an important point of human being aspects of information and technology. Generally, library management and security are increasingly engaging in dangerous online activities such as social networking, blogging and instant messaging with a considerable number of them unaware of their exposure management security risks while doing so.This review will explore the information management and security awareness, compare between the natural and intervention studies based on the previous research, also make the comparison between developed communities and developing countries because these countries have some different cultures that make different perspectives about information management and security awareness.

The higher the information management and security awareness will impact the better practice in human life both in the university library and in the government area, notwithstanding that both library information management and security awareness programs seek to manage risk by influencing individual behaviour. The study discuss the implications of biases on formulating

ISSN: 3428-0009

risk perceptions, shaping information management and security behavior; challenges which includes lack of motivation and awareness, computer security risks, inadequate use of technology, and propose a set of recommendations for designing management and security awareness program so as to accommodate management and security decision – making through human aspects such as demography psychograph, and self-efficiency and its effect on library information management and security awareness.

Information system security is strongly related to the concept of risk. Accordingly, risk is an event that may negatively affect the accomplishment of business objectives. The International Organization of Standardization (ISO) defines risk as the potential that a given threat will exploit vulnerabilities of an asset or group of assets. The impact of the relative severity of the risk is proportional to the business value of the loss or damage and the estimated frequency of threat. In general, the principal reasons for providing IS security may include protection of resources, maintaining management control, ensuring safety and integrity, implementing policies and laws, and attaining operational advantages and economies. Security failures can be costly for any institution. Losses may be suffered as a result of the failure or as a result of the cost incurred for recovery, followed by more cost to secure systems and prevent further failures. It is worth noting that library management system also tend to think of IS security as a second priority compared with their own efficiency or effectiveness matters because these have a direct and material impact on the outcome of their work andhave investigated different aspects of cybersecurity, and they asserted that although information security and cybersecurity have substantial overlap, these two concepts are not totally analogous.

Way forward

ISSN: 3428-0009

The general definition of information security comprises availability, integrity, and confidentiality. Cybersecurity incorporates extra measurements, which stretch out past the formal limits of information security, incorporating human in their own ability and society on the whole. It tends to be harmed or influenced; while this is not really the situation with data security, where harm is constantly circuitous. The security objectives cannot be met by technical and procedural protection only; an educated security attitude of library staff, management, and external IT users and partners is also vital to ensure effective IS security. As highlighted in previous studies on IS security have focused on software for detecting IS security abuses, the measures for preventing IS security abuses, perceptions of IS security adequacy. IS security planningmodels for management decision-making? IS security approaches can be classified into two categories. Studies which consider IS security awareness to mean attracting users' attention to IS security issues, or studies which consider IS security awareness to mean users' understanding of IS security and, optimally, committing to it. The need to promote IS security standard within an organization requires IS security awareness training. All the users should be aware of disciplinary actions resulting from non-compliance with the university library IS security procedures. Previous study suggests that the university librarymanagement and security culture must be improved by taking human behavior into account Louis (2017). It also suggests that each user should be informed, through IS security awareness, of his role in protecting information assets. Also discussed the implementation of continuous IS security awareness training program as part of the corporate asset protection program.It arguedthat organizations should introduce IS security awareness and make their ethical policy clear to their clientele and ensure that strong deterrents are in place. It furtherargues that the incompetence of users who underestimate the dangers inherent in their actions represent the biggest IS security problems. An efficient IS security awareness program can overcome this problem.

ISSN: 3428-0009

The university libraries are better prepared to screen their information security awareness position, their limits and the day by day weights influencing the library information management system.The information security focus areas included in this library information management and security policies are password management; use of email, the Internet and social networking sites; mobile computing; and information handling. However, the maturity levels of these elements varied among focus areas due to a lack of information security policies awareness and compliance among library users. Major causes of the occurrence of human errors include lack of knowledge or skills related to IS; thus, managing human error in any university library is vital, and errors must be taken as a serious threat. Responsibility, trust, communication, and co-operation are said to be the four cornerstones of an engaging security culture. Using an approach that motivates and empowers students to play an active role in security is important towards achieving awareness and positive behaviors. Awareness output should be tailored to university context, addressing specific management and security needs on an on-going basis to reinforce awareness, embedding security practices into the normal routine of management and security-minded culture.

When discussing management and security of library information management, the problems that occur are related to convenience. Management, Security and convenience are issues faced the most by each institution that implements a security system. In this case, there is a management and security paradox, Human vulnerabilities are a giant source of information security risks and thus the results of breaches in information security end up in university library students' losses and even to crimes. People will only facilitate in preventing security breaches, if they are aware of the risks, and are taught secure behaviors as a part of their traditional work training.

ISSN: 3428-0009

To ensure appropriate information security and protect the Smartphone from regular attack, library may consider; Raising a strong awareness campaign on the use of Smartphone's by criminals to attack information; Smartphone users should avoid completing online transactions requesting account information, password, credit numbers and other information without secured connection "https" in the website address; Unknown website such as music, video, sport, etc. sites may be avoided because of their exposures to malware;Phone makers should develop reliable surveillance software to help identify criminals' activities on a targeted phone; Appropriate policies and strategies should be put in place by government to discourage information security breach attempt at all times and real mechanisms to emphasis and combat cybercrime should be put in place to check and punish cyber criminals.

Giving training is one of the factors that increase human's level of satisfaction. Policies need to be readily accessible or available to library staff and users to ensure that they will not be ignored. It ought to be clear to what their actual role and responsibilities are regarding security. University libraries must address all possible human errors while writing IS because such errors can be critical for any environment if not handled competently.Information security management should be introduced as a degree course in the universities etc.

Conclusion

Information security is imperative, demanding and complex. In all universities, information security is essential to teaching, learning and research. Any threat or attack to library information resource is catalyst to development.The management and security of sensitive data is only as strong as the weakest link, which often turns out to be the human user and not the firewall. This makes the users' awareness of the data created as well as the risk connected with data breach critical. Based on the discussion, the focus has always centered on training users

ISSN: 3428-0009

about specific risk areas. Developing countries must see information security threat and attacks as catalyst to development and fight it with all zeal. The use of Smartphone is good. But to ensure an information secured society, there is need for collaborative initiative between stakeholders in promoting a culture of information secured environment as a basis for sound development.The implication of this study is that information management and security awareness is the key to mitigating management and security threats caused by human weaknesses.

The challenges related to information management and security that is faced on a day after day must be understood and resolved. This suggests that management and security functions should be substantive and as very little intrusive as possible. Additionally, management and security, policies must be comprehensible and straightforward to locate. Students' education about the importance of management and security awareness ought to be a priority of the university library.

References

Albrechtsen, E., (2007) ―A qualitative study of users' view on information security, Comput. Secur., vol. 26, no. 4, pp. 276–289.

Allam, Flowerday S. S. V., &Flowerday E.(2014), Smartphone information management and security awareness: A victim of operational pressures, Comput. Secur., vol. 42, no., pp. 55-65,.

Alqahtani, F. H. (2017).Developing an Information management and Security Policy: A Case Study Approach, ProcediaComput. Sci., vol. 124, pp. 691–697,

Arachchilage N. A. G.& Love S., (2014)Security awareness of computer users: A phishing threat avoidance perspective,Comput. Human Behav., vol. 38, pp. 304–312,.

Arachchilage, N. A. G. & Love, S. (2013). A game design framework for avoiding phishing attacks,‖Comput. Human Behav.,

European Network and Information Security Agency {ENISA) {2015)

ISSN: 3428-0009

Garcia, J. {2014} Smartphones as Tools for Education: Getting Smart with Smartphone. http://www.ecyclebest.Com (Retrieved 10 January, 2014)

Goodhue, D. L. & Straub D. W., Security concerns of system users: A study of perceptions of the adequacy of security,Information management., vol. 20, no. 1, pp.

Jatto, A. (2014) Effects of Spyware on information security. International Journal of Science Innovations and Development 4(1) pp 74 – 81

Kritzinger, E., Cyber Security for home users: A New Way of Protection through Awareness Enforcement,pp. 1–15.

McCormac, A., Parsons K., Butavicius M., and Ferguson L., Human Factors and Information Security: Individual, Culture, and Security Environment,‖ Sci. Technol, p. 45,.

Metalidou, E., Marinagi C., Trivellas P., Eberhagen N., Skourlas C., & Giannakopoulos G., (2014) The Human Factor of Information Security: Unintentional Damage Perspective,Procedia - Soc. Behav. Sci., vol. 147, pp. 424–428,.

Mylonas, A., Kastania A.,&Gritzalis D., (2013) Delegate the smartphone user? Security awareness in smartphone platforms, Comput.Secur., vol. 34, pp. 47–66,.

Rooney, B. (2011) Malware is Posing Increasing Danger, Wall Street Journal 5 (23) pp. 1 - 5

Vila, M. (2014) Wireless Phones http:/www.verzonwireless (Retrieved 3rd December 2014)

Von Solms, R., J. V. N. & security, (2013), ―From information security to cyber security, Elsevier.