http://dx.doi.org/10.5455/sf.106118

Science Forum (Journal of Pure and Applied Sciences)

journal homepage: www.atbuscienceforum.com

Impact of the cybersecurity system on information keeping: A study of selected tertiary institutions in the northwest of Nigeria

Sulaiman Usman Dan-ghani, Sahalu Balarabe Junaidu, Afolayan A. Obiniyi, Mustapha Aminu Bagiwa, Garba Aliyu*

Department of Computer Science, Ahmadu Bello University Zaria, Zaria, Nigeria

ABSTRACT

This study examined the impact of cybersecurity policies on information protection in some of the tertiary institutions in the northwest of Nigeria. The research was conducted based on two research questions and the use of a descriptive survey design. The data used was primary data gathered by a structured questionnaire. The population of the study consists of 3,257 participants and 356 were sampled using Taro Yamane's formula. The data gathered was analyzed by employing Z-test with the help of Statistical Package for the Social Sciences software. The findings revealed that the cybersecurity system has a notable consequence on staff information protection in the chosen tertiary institutions in northwest of Nigeria and that the cybersecurity system has a notable impact on students' information (database) in the chosen tertiary institutions. From the analysis, the findings recommend that tertiary institutions should have effective and efficient cybersecurity to secure vital information in tertiary institutions.

ARTICLE INFO

Article history:
Received 10 May 2020
Received in revised form
30 July 2021
Accepted 01 August 2021
Published 12 October 2021
Available online 12 October 2021

KEYWORDS

Tertiary institutions
Cybersecurity
Information
Security
Protection

1. Introduction

The infiltration of information systems promotes effective access to information, and because of this secrecy is at a high risk; uncertainty, invisibility, and deception of criminal traces have become issues of spacious concerns. The obscurity of the cyberspace makes identity tracing very difficult, which presents obstacles in disclosure and investigations. It is clear that software runs the world as we are in the period of fast globalization and technological headway wherein the Internet has become everything (Pocar, 2014). For over some decades, software has penetrated new areas as it interconnects individuals and systems, gets more intelligent, progressively more complex, and increasingly self-sufficient (without human intervention). This is lacking a definite plan step, but is yet predictable, with expected development for monetary increase, enhancements in personal satisfaction, and answers for the issues we face and the chances we look for (Gordon and Ford, 2016).

According to Snyder (2011), cybersecurity is currently viewed as a significant part of people and families, just as organizations, governments, institutions of learning, and our industry. It is a collective responsibility of every individual to inform people who are not aware of Internet fraud. As far as financial security goes, it is critical to make sure that our financial information is safe as it can compromise our money-associated reputation. The Internet is significant and valuable to educational institutions, which furnishes a lot of learning possibilities with numerous Internet

* **Corresponding author** Garba Aliyu ✉ algarba@abu.edu.ng ✉ Department of Computer Science, Ahmadu Bello University Zaria, Zaria, Nigeria.

risks. There is an indispensable need for online users to learn how to be protected from online extortion and malicious theft of their identity. The speedy development of technologies is additionally making cybersecurity more difficult as we do not present lasting solutions for the concerned Internet predicament (Wall and Williams, 2011). Even though we are effectively battling and introducing different frameworks or technologies to ensure our Internet and information is safe, they give us no permanent protection. However, more trustworthy security intelligence and suitable tactics can assist with protecting intellectual property including business confidences and to overcome or diminish financial and reputation loss. The government agencies store a large amount of information in the cloud but the major issue remains on how the Internet becomes the main target for attack. More often than not, governments face challenges because of bad infrastructure, absence of awareness, and poor funding. This requires the need to offer dependable types of assistance to society, keep up sound communications of the citizen to government and assurance of confidential data (Kshetri, 2010).

According to Duan and Chen (2016), amongst the most uncertain elements of cybersecurity is the steadily emerging nature of security risks. Therefore, this research tries to investigate the impact of cybersecurity system on information storage in some selected tertiary educational institutions in the northwest of Nigeria. This study aimed to measure the impact of the cybersecurity system on staff and students' information storing in some institutions in the northwest of Nigeria. Moreover, this research is guided by questions on how a cybersecurity system affects staff and students' information storing in the institutions.

1.1. Hypotheses

The following null hypotheses guided the study:

H_{01}: A cybersecurity system does not have a significant effect on staff information keeping in selected tertiary institutions in northwest of Nigeria.

H_{02}: A cybersecurity system does not have a significant effect on students' information (database) in the selected tertiary institutions in northwest of Nigeria.

2. Literature Review

2.1. Conceptual review

2.1.1. Cybersecurity

Cybersecurity is the act of securing systems, Internet, and applications from attacks. These attackers typically plan on getting to, changing, or wrecking sensitive data. Monies are extorted or cause interruption of the normal flow of business activities in a bid to get or have access to some sensitive information. Realizing efficient cybersecurity models is expressly challenging now because there are many devices that are more vulnerable than humans, and intruders are becoming more advanced in cybercrime. Cybersecurity strengthens Internet systems, which comprise hardware, software, and information, from cyberattacks (Ngbokwe, 2012). In a computing setting, security encompasses cybersecurity and physical security. Industries use these to protect unauthorized users from having access to data centers and other related devices over the Internet. Information security is intended to preserve the confidentiality, integrity, and reliability of data (Tonge and Kasture, 2013).

2.1.2. Cybercrime

Every individual expert, which includes technical, lawyers, police, economic and financial crimes commission and criminologists, among others, understands the idea of cybercrime differently (McCullagh and Chantler, 2010). It is progressively hazy whether cybercrime alludes the legitimate, sociological, technological, or lawful parts of crime, and a universal meaning stays tricky (Kshetri, 2010). Investigators have endeavored to construct the fundamental components of cybercrime with a contracted agreement (Gordon and Ford, 2016). The maltreatment of information technology or the Internet by intruders reciprocally allude to cybercrime, computer crime, and other computer crimes (Goodman and Brenner, 2012). However, these terms are not interchangeable (Chik and Bartholomew, 2011). Following this definition, cybercrime is simply a subset of traditional crime where information technology is applied as a means or device to perpetuate common criminal offenses (Zhigang, 2011). This definition adheres to the rudiments of legal understanding applied to regular criminal offending. Lawmakers should be attentive to circumvent forming legitimate kinds of cybercrime offenses by tailoring laws to satisfy innovations in technology.

3. General Understanding of Cybersecurity

3.1. Growth in cyber crime

Virtually, all sectors now have embraced information technology to ease their daily activities through automation. By the end of 2019, over 4.39 billion people were using the Internet worldwide, and the percentage

is increasing rapidly. Momentarily, our lives seem incomplete without the Internet, mobile phones, and computers. Information is stored digitally and conveyed through communication channels. Government and other financial businesses also accept the Internet as a means to carry out financial transactions. This necessitates the circumstances of acquiring secured Internet and having reliable devices to prevent intrusion that may cause damages. According to a report, nearly 1,00,000 viruses/worms are running around every day and among which 10,000 are identified as different and unique (Snyder, 2011).

4. Theoretical Framework

Kwon and Zmud (1987) introduced the theory of model of IT implementation process (MIIP), which was later enhanced by Cooper and Zmud (1990). The model suggested a framework for informing and adapting research based on innovation, changes in regulations, and technological spread. Kwon and Zmud's (1987) first model introduced six stages, including initiation, organizational adoption, adaptation, acceptance and adoption, routinization, and diffusion. MIIP seems to be an extremely embracing model than most of the models so far recognized. Aside from concentrating on the six phases from appropriation to dissemination of IT, it additionally analyzes mediating factors, for example, the technology being utilized. MIIP has all the earmarks of being decent hypothetical support for ICT adoption and usage studies. However, it is dubious if this can be utilized to adequately give a hypothetical system to a study including electronic extortion and detection.

4.1. Empirical studies

Snyder (2011) carried out a study on the importance of cybersecurity in the government house in Thailand. This research was carried out to answer three research questions and use a descriptive survey design. The population of the research consists of 300 staff and 150 were used as a sample using random sampling of 50% of the population. The data were collected through a structured questionnaire, which as primary data for the research. The data were analyzed by applying simply percentage and Z-test with the help of Statistical Package for the Social Sciences (SPSS). The findings revealed that cybersecurity helps in the protection of government's vital information and prevents unauthorized financial accessibility.

Gordon and Ford (2016) carried out a research on the effect of cybersecurity on the information security considering 16 manufacturing firms in Australia. The population of the study consists of 1,200 staff and 400 were taken as sample using the random sampling method. The data used were primary data collected through structured questionnaire. The data were analyzed using simply percentage and one-way analysis of variance with the help of the statistical software SPSS version 20. The findings revealed that cybersecurity has a significant impact on information security, especially on the manufacturing firms.

5. Methodology

5.1. Research design

The research used adopted a descriptive survey design. Descriptive survey research is centered on people, attitude, belief, motivation, behavior, and opinions. Nworgu (2015) recommend the descriptive survey as more appropriate especially for studies seeking individual opinions, attitudes, and perceptions in their natural setting.

5.2. Area of the study

This research was carried out in the northern part of Nigeria, particularly northwest. The states includes Kaduna, Kano, Katsina, Kebbi, Jigawa, Zamfara, and Sokoto. The northwest is part of the six geopolitical zones of Nigeria. Hence, the study was carried out in the tertiary institutions in the northwest of Nigeria as shown in Table 1.

5.3. Sampling procedure

The sample size was obtained through the use of Taro Yamane's formula for determining the sample size. This is given as follows:

$$n = \frac{N}{\left[1+N(e)^2\right]}$$

where n = sample size; N = population of interest (which is 3,257);

e = error estimate/level of significance, which is normally 5%.

By solving $n = \frac{3,257}{\left[1+3,257(0.05)^2\right]}$

$n = 356$

5.4. Reliability of the instrument

The pilot study was conducted using 25% of the sample size of the study, which is 89 copies of the questionnaire. Eventually, 75 copies were retrieved

Table 1. Population distribution of the tertiary institution.

	Tertiary institution	Population of staff
1	Ahmadu Bello University Zaria Kaduna	278
2	Yar'aduwa University Katsina	229
3	Federal University Dutsenma	201
4	Al-kalam University Katsina	241
5	Bayero University Kano	126
6	Maitama University Kano	232
7	University of Technology Wudil, Kano	139
8	Federal University Dutse	208
9	Jigawa State University Dutse	116
10	Federal University Gusau	221
11	State University Gusau	139
12	Nigerian Defense Academy Kaduna	319
13	Federal University Kebbi	211
14	State University Kebbi	144
15	Federal University Sokoto	279
16	State University Sokoto	174
	Total	**3,257**

Source: Field Survey, 2018.

Table 2. Reliability statistics of the study.

Cronbach's alpha	No. of items
0.880	75

Source: Field Survey (pilot study), 2018.

Table 3. One-sample Kolmogorov–Smirnov (Z-test) of staff information.

		Cybersecurity/ information keeping
N		5
Normal parameters [a,b]	Mean	71.200
	Std. deviation	69.770
	Absolute	0.029
	Positive	0.029
	Negative	−0.139
Kolmogorov–Smirnov *Z*		0.492
Asymp. Sig. (2-tailed)		0.010

[a] Test distribution is normal.
[b] Calculated from data.

representing 21% of the sample size. The result obtained is shown in Table 2.

From the result obtained, the reliability coefficient was 0.880, which if converted into percentage is 88%. This signifies that the instrument is reliable and capable of eliciting consistent result. The data collected were analyzed using Z-test.

6. Data Presentation and Analysis Test of the Hypotheses

6.1. Decision ruleWe accept the null hypothesis when the probability value is greater than the alpha value, otherwise we reject it.

6.2. Hypotheses I

H_0: A cybersecurity system does not have a significant effect on staff information storing in tertiary institutions.

H_1: A cybersecurity system has a significant effect on staff information storing in tertiary institutions.

The result of the analysis in Table 3 suggests that the probability value (0.010) is lesser than the alpha value (0.05). This suggests that, therefore, we can accept the alternative hypothesis and conclude that a cybersecurity system has a significant effect on staff information storing in selected tertiary institutions in the region under study.

6.3. Hypotheses II

H_0: A cybersecurity system does not have a significant effect on students' information (database) in the tertiary institutions.

Table 4. One-sample Kolmogorov–Smirnov (Z-test) of student information

		Cybersecurity/students information
N		5
Normal Parameters [a,b]	Mean	71.200
	Std. deviation	66.000
	Absolute	0.129
	Positive	0.129
	Negative	−0.239
Kolmogorov–Smirnov Z		0.492
Asymp. Sig. (2-tailed)		0.001

[a] Test distribution is normal.
[b] Calculated from data.

H_1: A cybersecurity system has a significant effect on students' information (database) in the tertiary institutions.

The result of the analysis in Table 4 reveals that the probability value (0.001) is lesser than the alpha value (0.05). This suggests that, therefore, we can accept the alternative hypothesis and conclude that a cybersecurity system has a significant effect on students' information (database) in the selected tertiary institutions in the regional part of the country under study.

7. Conclusion and Future Work

Having carried out the analysis, this research concludes that the cybersecurity system has a significant effect on staff information storing and on students' information (database) in the selected tertiary institutions in northwestern part of Nigeria. From the analysis, the findings recommend that tertiary institutions should have effective and efficient cybersecurity to secure vital information in tertiary institutions. However, this research can be extended by considering other regions, where the level of vulnerability can be accessed and appropriate decision-making can be made by the state and federal governments. In addition, this research focused on public, state, and federal universities. This suggests that private universities have to be considered and possibly compare the level of security measures put in place.

References

Chik WB, Bartholomew W. Challenges to criminal law making in the new global information society: a critical comparative study of the adequacies of computer-related criminal legislation in the United States, the United Kingdom and Singapore, 2011. Available via http://www2.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Accessed 10 November 2016).

Cooper RB, Zmud RW. Information technology implementation research: a technological diffusion approach. Manage Sci 1990; 36(2):123–39.

Duan O, Chen T. Cybercrime: conceptual issues for congress and U.S. law enforcement. Congressional Research Service, Washington, DC, 2016.Goodman N, Brenner M. Cyber security in Africa: an assessment. Georgia Institute of Technology, Atlanta, GE, 2012.Gordon M, Ford E. Challenges of cyber security and it implication on information system. J Comput Eng 2016; 2(12):67–75.

Kshetri C. Understanding cybercrime: phenomena, challenges and legal response. International Telecommunications Union, Geneva, Switzerland, 2010.

Kwon TH, Zmud RW. Unifying the fragmented models of information systems implementation. In: Boland RJ, Hirschheim R (eds.). Critical issues in information systems research, Wiley, New York, NY, pp 227–51, 1987.

McCullagh V, Chantler W. Impact of cybercrime: issues and challenges. Int J Eng Sci Emerg Technol 2010; 6(2):142–53.

Ngbokwe T. Vulnerability assessment of cybersecurity for SCADA systems. IEEE Trans Power Syst 2012; 23(4):1836–46.

Nworgu BG. Educational research: basic issues and methodology. University Trust Publishers, Enugu, Nigeria, 2015.

Pocar P. Tracking and tracing cyber-attacks: technical challenges and global policy issues. Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, 2014.

Snyder Y. Mapping and measuring cybercrime. OII Forum Discussion Paper No. 18, University of Oxford, Oxford, UK, 2011.

Tonge E, Kasture D. Telecommunication fraud detection using data mining techniques. Masters Dissertation, University of Porto Faculty of Engineering, Porto, Portugal, 2013.

Wall V, Williams K. Cybercrime and information welfare. In Transnational Crime Conference. Australian Institute of Criminology, Canberra, Australia, pp 2–19, 2011.

Zhigang L. China tackles advance fee fraud. J Inf Law Technol 2011; 2(1):1–20.