E-ISSN: 1115 - 8530 P-ISSN: 3026-8958
MPRI-JFRBD | INTERNATIONAL JOURNAL OF FINANCIAL RES. AND BUSINESS DEVELOPMENT
VOL. 10 NO. 7 – OCTOBER, 2025

CYBER SECURITY AND ORGANIZATIONAL SURVIVAL

ASSOC. PROF. PETERSON NWOKORIE
Department of Management, Faculty of Management Sciences, Imo State University, Owerri
DOI: https://doi.org/10.70382/mejfrbd.v10i7.074

Abstract

This study examined Cyber security and organizational survival. Survey research design was used and questionnaire served as the instrument of data collection. The data collected were presented in tables and analyzed using mean statistic, and Pearson correlation with the aid of SPSS version 21.0 (at 0.05% level of significance). It was discovered that there is significant relationship between Cybersecurity Training (CT) and output maximization in the bank; and Cybersecurity Awareness (CA) affects organizational effectiveness in banks. The study concludes that Nigeria has greatly suffered in Cyber-attack. Based on the findings of this study, it was recommended that organizations should build awareness of security issues across the internet community and promote cyber security awareness; and to improve cyber security posture organizations should train their employees on the major aspects of cybercrime and strategies for managing, reducing and stopping.

Keywords: Cyber security, organizational survival, Training, Awareness, organizational effectiveness, output maximization

Introduction

Technology adoption is driving business growth and innovation in Nigeria, at the same time it is exposing the country to new and emerging threats. Cyber-terrorists, spies, hackers and fraudster are increasingly motivated to target our ICT infrastructure due to the increasing value of information held within it and the perceived lower risk of detection and capture in conducting cybercrime as compared to more traditional crime. According to Yakubu(2019), internet usage has been rapidly rising in Africa, as more people connect to the inter-web mostly through their mobile phones. This increased use has created a new challenge for the continent in potential attack vectors at

both individual and organizational level. Juwah (2015) opine that with the increasing availability and utilization of internet facilities, threats in the cyber space have also escalated dramatically. Criminals are invading homes and offices not by breaking doors and windows but by breaking into laptops, Personal Computers and wireless devices through the internet. Therefore, there is need for cyber security.

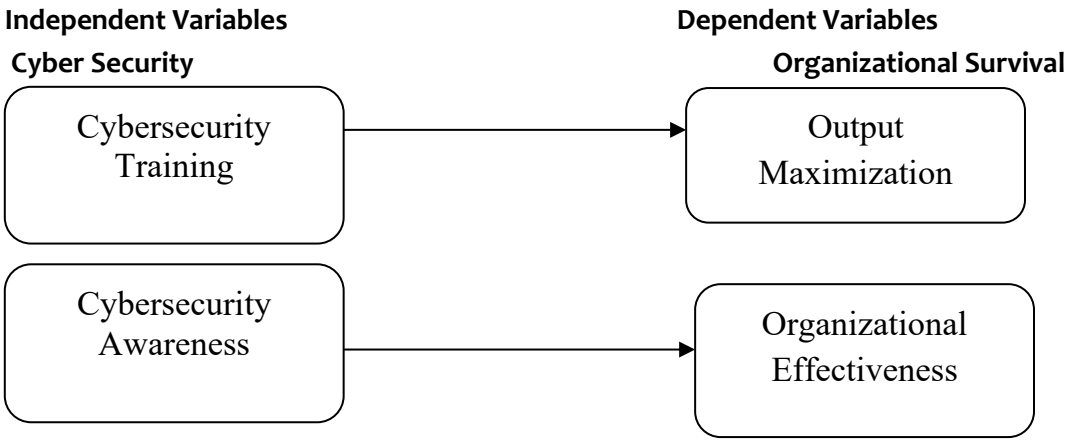
Cyber security is one of the great human rights issues of our time (Direv and Hu, 2007). Cyber security is not only an issue for "Internet users" but for all citizens. Even someone who has never been online is directly affected when a retail company they frequent (for example, Target or Home Depot) experiences a massive consumer data breach, when their television potentially becomes a surveillance tool or when they are denied medical care because of a ransom were attack that cryptographically locks medical records and otherwise disables health care provider systems. All people and all societies are now directly affected by the security of digital systems (Schneier and Bruce, 2016). Debates on cybercrime and cyber security tend to concentrate around dramatic events such as the defacement of popular online spaces, sensitive information leaks or diffusion of particularly infectious malware (Schneier and Bruce, 2016).

This work focuses on training end users with or no professional cybersecurity training for they have the greatest need to improve in the organization. Other issues in cyber crime is awareness programs provide guidelines such as using strong passwords, use a different password for each account, do not post the password on the computer screen and so on, but fail to educate the user on other issues, such as interpreting warning messages and responding appropriately. Furman, Theofanos, Choong and Stanton (2011) remarks, "We're all familiar with the obscure "certificate warnings" that our Web browsers occasionally grace us with – these warnings are entirely indecipherable, un-actionable, and thus routinely ignored." This suggests that cybersecurity training programs may need to go beyond simple awareness education. In all, the work focused on cyber security and organizational survival.

Statement of the Problem

Cyberspace have ushered in new opportunities with its security challenges. The role of sovereign nation-states in addressing cyber security is in a state of flux. On the one hand, these states have an interest in preserving the security of critical infrastructure. On the other hand, they are not cyber resilient enough. Studies have shown that the internet has overtaken the television in the number of audience at prime time, totaling over two billion users worldwide with well over 200 million websites(Akpan, 2022). Despite the growing number of Nigerian users running into millions, the country's leaders are not paying enough attention to various activities in the cyberspace. As cyber threats become more

complicated, the role of institutions such as computer security incident response teams (CSIRTs) becomemore important. This study therefore focused on cyber security and organizational survival.



Source: The Researcher's Desk, 2025

Objective of the Study

The major objective of this study focused on cyber security and organizational survival. The specific objectives of this study are to:

1. find out the relationship between Cybersecurity Training (CT) and output maximization in the bank.
2. determine the extent Cybersecurity Awareness (CA) affects organizational effectiveness in banks.

Research Questions

The research questions for this proposal are:

1. What are the relationship between Cybersecurity Training (CT) and output maximization in the bank?
2. To what extent does Cybersecurity Awareness (CA) affects organizational effectiveness in banks?

Research Hypotheses

This study is guided by the following null hypotheses.

Ho1: There is no significant relationship between Cybersecurity Training (CT) and output maximization in the bank.

Ho2: Cybersecurity Awareness (CA) does not affect organizational effectiveness in banks.

Concept 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(Eminagaoglu, Ucar and Eren, 2009). According to Akpan (2022), 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 Confidentiality. 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). Then security network guards against unauthorized intrusion as well as malicious insiders. Ensuring security network often trade-offs requires. Example, This makes passwords more subject to different kinds of attacks. To access passport such as extra logins might be necessary but slow down productivity tools used to monitor network security generate a lot of data so much that end users often miss valid alerts(Ike, 2019). To help manage network security monitoring and security teams are increasingly using machine learning to flag unusual traffic and alert to threats in real time.

Organizational Survival

Organizational survival is the ability of an organization t achieve its goals, remain in the system, and continue to provide its products/services(Namusonge, Willy and Olawoye, 2022). Organizational survival is the extent to which a firm achieves its business objectives, and attracts more customers for business growth. Survival covers customer patronage, retention, acquisition, satisfaction and all customer based variables. Suth and Ginsberg (2010) in Ike (2019) opine that Organizational survival is the process of improving some measure of an enterprises success; it can be achieved either by boosting the top line

or revenue of the business with greater product sales or service income, or by increasing the bottom line or profitability of the operation by minimizing costs.

Strategies to Strengthen Cyber Security and Organizational Survival in Nigeria

Based on the World Economic Forum (2012) research findings, most Nigerian organisations are ill-equipped to respond to information security threats. Although there are different initiatives (regulators, government and private organisations) in place set out to address information security issues in Nigeria, these initiatives cannot adequately address the current information security issues. Public and private organisations 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 organisations 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 wellfunctioning network of Computer Emergency Response Team at the national level. The organisation of cyber incidents simulations, putting in places a well-defined policy on Critical Information Infrastructure Protection (CIIP) with the aim of strengthening the security and resilience 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.

Measuring cyber security for survival of organizations

There are many indices which could be used to measure cyber security for survival of organizations. They include:

Cybersecurity Training (CT)

In business environments, the need for the implementation of security countermeasures such as CT has been emphasized and recommended to reduce computer abuse (Vanson and Bourne, 2012). Security policies form the basis for security education training and awareness (SETA). CT sessions, in general, are aimed at informing the users about unacceptable system use and penalties for noncompliance (Namusonge, Willy and Olawoye, 2022). CT is defined as those activities that impart specific cyber skills such as safe internet browsing, encryption, decryption and system manipulation (Kaplan, James and Tucker, 2015), to make security decisions (Furman et al. 2011). The ultimate goal of CT is to impart knowledge and skills such as vulnerability analysis and mitigation, intrusion detection, and incident response, to be less susceptible to social engineering. Human always has weakest element in the cybersecurity program

Training developers to code securely, training operations staff to prioritize a healthy security posture, training end users to spot phishing emails and social engineering attacks, and the cybersecurity begins with awareness with all the companies with experience some kind of cyber attack even if they have robust controls in place. Likewise, an enterprise must implement the essential elements of cybersecurity for such care and maintainingsecureauthentication practices and storing sensitive data where it is openly accessible to the end user. The End-user training is recognized as an essential component of the steps necessary to improve cybersecurity compliance, and consequently, cybersecurity posture. Antecedents of cybersecurity compliance in both the home and organizational context have been studied. Among the individual factors that have been examined are cybersecurity awareness, self-efficacy in information security and, to a lesser extent, cybersecurity skills. Each of these variables is potentially a mediator between cybersecurity training and compliance. Research has not examined either the mediating role of these three factors, nor has it reviewed the relative effectiveness of these measures in achieving compliance.

Hence the research questions that will be pursued in our research are: 1. What factors mediate the relationship between cybersecurity training and compliance? 2. What is the relative effectiveness of each factor in improving compliance? 3. How does the nature of training affect each of the mediating variables? A good cybersecurity strategy is to go beyond these basics devices. The Sophisticated hackers can circumvent most defenses, and the attack surface the number of ways or "vectors" an attacker can gain entry to a system is to companies. The It was expected that with these technology advances and the criminals and nation-state spies now threaten most the ICA cyber-physical systems such that most cars, power plants, and the medical devices and hardware and software devices. Similarly, the trends toward hardware and software devices cloud computing,

bring your device (BYOD) policies and the burgeoning internet of things (IoT) creates new challenges. Defending these systems has never been more effective.

Cyber Security Awareness (CA)

We can define as the state of being cognizant of performing secure tasks on a computer (Cassim, 2011). Studies have focused on different aspects of awareness. For instance, some have examined knowledge of computer usage policies (e.g., Obama, 2009), others have examined security countermeasures (e.g., D'Arcy et al. 2009) and so on. The multiple aspects collectively include comprehensive information about general guidelines of information security, education on security risks and its consequences on cybersecurity threats, and tracking internet usage for abnormal activities (Greenwald. 2014). All awareness aspects listed in table-3 can be categorized into three dimensions The approaches to information security include both technical, non-technical solutions as they Cyber attacks come a long way from the email viruses well, as Passwords are the most commonly used method of authenticating users to information systems criminals adapt to changing, The IT security experts whose job it is to keep our data safe in any organization.

Theory of Cyber Risk

This theory was developed by Dick in 1970. 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 Onuorah, Okeke, and Ibekwe (2019), 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.
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 connected devices such as medical devices or industrial systems.
External Unintentional: Similar to the internal unintentional, 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.

Physical Security Theory

This theory was developed by Dan in 1989. The Physical security and Cyber threats aren't the only ones employees need to look out for. They also play a role in keeping sensitive information of the organization protected and leaving a mobile device, or its most risk end users end up committing. If someone were to wipe thephone of an employee's and log into their computer, all of their data and information would be accessible in their device. Below are the few best practices to help the end user to increase their physical security within the organization Lock your device before and after you leave your desk. In Windows users, press and hold the Windows key, then press the "L" key. For Mac users, press Control + Shift + Eject (or the Power key) at the same time. Documents should be locked at the cabinet (Store).Should avoid having sensitive information floating around on their desk (Employees). The before or end of the day, they leave their office unattended; it's always a good idea to stow company documents and the like into a lockable safe or cabinet. Properly discard the information. When it comes to getting rid of those documents or files, be sure properly shred and discard them.

Theory of Cybersecurity Compliance

The theory was developed by Herath and Rao (2009), and encouraged by Johnston and Warkentin 2010. The End user is a specific case of cybersecurity behavior in which end users conformity with the safe and secure rules and policies, and comply with a recommended of action (Johnston and Warkentin 2010, Herath and Rao 2009).The training programs are designed to achieve goals that meet instructional needs. It is counterproductive to launch training without a thorough assessment of role-relevant

tasks, behaviors, and environment (Wiley, 2015). Table-1 provides a summary of a sample of studies in which CC is the dependent variable. Several points can be seen in the table. First, cybersecurity compliance has been studied both in organizational and home context. In an organizational context, the studies have been conducted at both corporate and individual level of analysis. In the home context, studies have been at a different level of analysis. The model that is being developed in our research is for the different level of analysis and should be applied in both the home and organizational context. Fortunately, there are already a number of organizations that have identified the need for continental coordination and increased cybersecurity awareness while the rest of the world is increasing its focus on cybersecurity through relevant policies, strategies, infrastructure, technology development and awareness campaigns, only a few African countries have cybersecurity policies and appropriate security response structures or agencies such as CERTs.

The full responsibility to engender organizational support and convene of SMEs whose collective competencies match the complex challenges posed by a need for the specific training. Organizations must systematically train employees an army of cybersecurity; not all employees will become cyber experts, employers can hold trained end-users accountable for cyber defense performance apropos of the roles they perform. This will teach the user that they are a target, on how to look out for and phishing, password, social engineering, handling of any sensitive data and device. The most effective way to deliver practical Cybersecurity awareness should reach all levels and inform all users of the internet – from vulnerable, school-going children to families, industry, critical national infrastructures, governments, and the African continent with its unique needs. This will enhance resilience against cyber crimes and attacks and inform African policy development but also prompt the establishment of appropriate organizations such as CSIRTs and collaboration mechanisms to secure the continent and join the efforts of the global community of responsible and secure internet users. Since security awareness has shown to be a barrier to securing information systems in a variety of organizations, it is essential to know that higher institutions like FSU have a role to play in ensuring that user awareness is promoted and appropriately implemented.

Empirical Review

The researcher used the following empirical studies to beef the study:

Yakubu (2019) investigated the Effectiveness of Cybersecurity Compliance in a Corporate Organization in Nigeria. Descriptive research was used in the study. Stratified random sampling was used to select a sample size of 96. Structured questionnaires were used to collect data. Descriptive and inferential statistics was used to analyze data. It found that

the Training can influence compliance by one or more of three causal pathways: by increasing cybersecurity awareness, by increasing cybersecurity proficiency (i.e., improve cybersecurity skills) and by raising cybersecurity self-efficacy. This includes an extensive review of the cybersecurity policies and competencies that are the basis for training needs analysis, setting learning goals, and practical training.

Akpan, (2022) studied critical Analysis of Cyber Security and Resilience in Nigeria. The population of this study consisted of all professionals in computer science, computer engineering and security agents who have been exposed to computer science. The study adopted descriptive survey research design while stratified random sampling technique was used in selecting the respondents. The instrument for data collection which was tagged "Cyber Security and Resilience Questionnaire" (CSRQ) was administered to the respondents and used for the study. The instrument passed through face and content validation using experts in computer science before the reliability test was conducted which produced the reliability coefficient of 0.92 proving the instrument to be reliable for the study. Data collected were analyzed using descriptive analysis and chi-square analysis. From the results of the data analysis, it was observed and concluded that Nigeria has suffered greatly in Cyber-attack and that the Cyber security and resilience has become useful tool to checking and stopping cyber risks.

Ike (2019) focused on effectiveness of cyber security in business and banks. Survey research design was adopted and questionnaire served as the instrument of data collection. The population of this is 178 which is made up of the entire management staff of banks used. Out of 178 copies of the questionnaire distributed, only 168 were returned and used. The data collected were presented in tables and analyzed by mean frequency. The study discovered that poor security leads to cyber crime.

Namusonge, Willy &Olawoye (2022) determined the impact of cyber crime on performance of firms in Lagos. It used survey and collected data through telephone interview. Methods of statistical analyses include mean, standard deviation, and Pooled, Random and Fixed regression models. The results of analysis indicated that ineffective cyber security leads to cyber crime.

Onuorah, Okeke and Ibekwe (2019) examine cyber security challenges and performance in Nigeria organization. The study adopts descriptive survey research design. The study was carried out in Anambra State using banks. The population of the study comprises 567 regular customers. The instrument for data collection is a structured questionnaire. The face content validity of the instrument was employee. The instrument was trial-tested on a representative sample of 20 employee randomly selected of Anambra State. In analyzing the data for the null hypotheses, Z-test was be used to test the hypotheses at

0.05 level of significance. It found a relationship between effective cyber security and bank performance.

Research Gap

The research gap in this work could be summarized in to:

Subject gap: None of the empirical studies covered the topic of this work. Some covered only independent variable (cybercrime), and other covers dependent variables (organizational survival).

Geographical or area gap: This study is using UBA, Union Bank, and Fidelity Bank Owerri, Imo State Nigeria. No work has been done using the same banks. Past studies only used firm within other parts of Nigeria and other used outside Nigeria.

Gap on the indices in the objective: Past studies did not use the same indices of measurement employed in this work. Such indices are Cybersecurity Training (CT) and Cybersecurity Awareness (CA) (for independent variable), and output maximization and organizational effectiveness (for dependent variable).

Research Design

Survey research design was used in this study. Survey research design was used because of its advantages in collecting primary data.

Population of the Study

Population is the total number of staff used in the area or organization of study. The population of this study is 110. According to Personnel Unit of the UBA, Union Bank, and Fidelity Bank Owerri, Imo State the staff population is 110 (**Source:** Personnel Unit of the banks, 2023).

Sample Size

Sample is necessary when the population is large. For the fact that the population is not large, the entire study population (i.e. 105) were used hence census enumeration methods were employed.

Sampling Technique

Considering the nature of the population, the researcher used census enumeration method, so as to study the entire population (110) – since it's not large – as sample size.

Questionnaire Administration

The questionnaire was used as the research instrument.

Validity of Research Instrument

The researcher used content and face validity methods to ensure that the research instrument was valid.

Reliability of Research Instrument

A pilot test was first conducted with a separate group who are not but possess similar characteristics with the respondents. The Pearson Product Moment Correlation Coefficient (PPCC) (r) was used to calculate the reliability index and the results gave 0.86% correlation.

Methods of Data Analysis

Data collected were analyzed using mean statistics. In the use of mean statistics, SA stands as Strongly Agreed, A stand as Agreed, D stands as Disagreed and SD stands as Strong Disagreed. More so, N entails the sample size, ∑x entails total number of observation, and x means mean. Also, Pearson product moment correlation coefficient, with the help of SPSS 21.0 and Microsoft Excel software, were used to test the hypotheses.

Data Presentation and Analysis

Not only that, out of 110 copies of questionnaire distributed, only, 100 copies were returned and used.

Section B: The Subject Matter

Table 1: Research question one: What are the relationship between Cybersecurity Training (CT) and output maximization in the bank?

S/N	Questionnaire Items	SA	A	D	SD	N	∑X	X	Dec
1	Cybersecurity Training (CT) will lead to employee effectiveness of cyber crime management	50	47	2	1	100	346	3.5	A
2	Cybersecurity Training (CT) will enhance output of workers	40	41	10	9	100	312	3.1	A
3	Cybersecurity Training (CT) will make the banks to put effective security check	51	46	1	2	100	346	3.5	A

Source: Field work, 2025

It is seen in table 1 that all the items were accepted. This is because item 1 has a mean of 3.5, item 2 has a mean of 3.1, and item 3 has a mean of 3.5 and item 4 has a mean of 3.4; hence all the items have mean scores more than 2.5 and above. It is therefore concluded that there is significant relationship between Cybersecurity Training (CT) and output maximization in the bank.

Table 2, research question two: To what extent does Cybersecurity Awareness (CA) affects organizational effectiveness in banks?

S/N	Questionnaire Items	SA	A	D	SD	N	∑X	X	Dec
5	Cybersecurity Awareness (CA) will make employees to inform customers on relevance security issues	47	43	6	4	100	380	3.8	A
6	Cybersecurity Awareness (CA) will lead to effectiveness of bank transaction	41	47	7	5	100	324	3.2	A
7	Cybersecurity Awareness (CA) is the major strategy for keeping employees well informed and achieving productivity of business.	55	39	4	2	100	347	3.5	A

Source: Field work, 2025

The above table 2 shows that all the items were accepted. This is because item 5 has a mean of 3.8, item 6 has a mean of 3.2, item 7 has a mean of 3.5 and item 8 has a mean of 3.1; hence all the items have mean scores more than 2.5 and above. It is therefore concluded that Cybersecurity Awareness (CA) affects organizational effectiveness in banks.

Testing of Research Hypotheses

Ho1: There is no significant relationship between Cybersecurity Training (CT) and output maximization in the bank.

H1	There is significant relationship between Cybersecurity Training (CT) and output maximization in the bank	Pearson Correlation= 0.81 Sig = 0.05 N=100	**VALID**

From the table above, the Pearson correlation is 0.81. It means that there is significant relationship between Cybersecurity Training (CT) and output maximization in the bank.

Ho2: Cybersecurity Awareness (CA) does not affect organizational effectiveness in banks.

H2	Cybersecurity Awareness (CA) affects organizational effectiveness in banks	Pearson Correlation= 0.80 Sig = 0.05 N= 100	**VALID**

From the table above, the Pearson correlation is 0.80. It means that Cybersecurity Awareness (CA) affects organizational effectiveness in banks.

Concise Table for Hypotheses Testing

S/N	Hypotheses	Statistical Tools Applied (Software R studio)	Result
H1	There is significant relationship between Cybersecurity Training (CT) and output maximization in the bank.	Pearson Correlation= 0.81 Sig = 0.05 N=100	**VALID**
H2	Cybersecurity Awareness (CA) affects organizational effectiveness in banks.	Pearson Correlation= 0.80 Sig = 0.05 N= 100	**VALID**

Discussion of Findings

The major findings of this study are discussed thus:

In line with the hypothesis one, this study revealed that there is significant relationship between Cybersecurity Training (CT) and output maximization in the bank. This finding is in line with Akpan (2022) that through training and retraining, employees will have the right information and know the best way to achieve security and reduce cyber crime.

The result of the hypothesis two revealed that Cybersecurity Awareness (CA) affects organizational effectiveness in banks. According to Ike (2019), if the issue of cyber crime must reduce, the employees and customers of financial institutions must be aware of its different types and how to secure the system.

Conclusion

Cyber crime is one of the major challenges affecting business survival, especially the banking sector. For that, there is need for effective cyber security so as to reduce the incidences of cybercrime. Based on the findings of the research work, it was concluded that Nigeria as can be found in other parts of the world, have suffered greatly in Cyber-attack. Cyber security and resilience has become useful tool to checking and stopping

cyber risks and with Cyber security and resilience our society is protected against cyber risk.

Recommendations

Based on the findings of this study, the following recommendations are made:

1. Organizations should build awareness of security issues across the internet community and promote cyber security awareness and ensure that all keys password to their documents are properly secured.
2. To improve cyber security standard organizations should train their employees on the major aspects of cyber crime and strategies for managing, reducing and stopping its occurrence.

REFERENCES

Akpan, E.E (2022). A critical Analysis of Cyber Security and Resilience in Nigeria.*World Atlas Journal of Library and Information Science*, 5(1)1. New York City.

Cassim, F. (2011) Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. CILSA XLIV 123-138.

D'Arcy, J., Hovav, A., &Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse a deterrence approach. Information Systems Research, 20(1), 79-98.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward PIT.Journal of the Association for Information Systems, 8(7), 23.

Eminagaoglu, M., Ucar, E., and Eren, S. (2009). The positive outcomes of information security awareness training in companies – A case study, InformationSecurity Technical Report, 14, 223-229.

Furman, S. M., Theofanos, M. F., Choong, Y. Y. & Stanton, B. (2011). Basing cybersecurity training on user perceptions. IEEE Security & Privacy, (2), 40-49.

Governance, (2015). Cybersecurity Strategy. Ministry of Information Communications and Technology.

Greenwald, G. (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York, NY: Metropolitan Books/Henry Holt.

Ike, J.S (2019). Effectiveness of cyber security in business and banks.*Journal of the Association for Information Systems*, 1(1):23.

Juwah, M. (2015). Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Information System Front 8 (5), 339–349.

Kaplan, B., James, D. and Tucker, N. (2015) Theory of deterrence and individual behavior. Can lawsuits control file be sharing on the Internet? Review of Law and & Economics 3 (3), 693–714.

Lamorde (2015). Education, poverty, political violence, and terrorism: is there a connection? Journal of Economic Perspectives 17 (4), 119–144.

Namusonge U., Willy E.Jand Olawoye, T.O (2022).The impact of cyber crime on performance of firms in Lagos.*Journal of Social Issues*, 2(1), 19-22.

Obama, B.H(2009). Remarks By The President On Securing Our Nation's Cyber Infrastructure, BH Obama, President of the United States of America; The White House, Office of the Press Secretary, available online from

Onuorah C.I, Okeke E.G, and Ibekwe, C.C (2019).Cyber security challenges and performance in Nigeria organization.*International Journal of Economics and Business Management, 1(2): 7-15.*

Ravi, D. (2012) How optimal penalties change with the amount of harm.*International Review of Law and Economics,* 15 (1), 101–108.

Schneier, D. & Bruce, C. (2016). Lessons From the DynDDoS Attack, Schneier on Security Blog, 8 November 2016, https://www.schneier.com/blog/ archives/2016/11/lessons_ from_th_5.html

Steffani, H. (2006). Do bad boys really get the girls? Delinquency as a cause and consequence of dating behavior among adolescents. Justice Quarterly 21 (2), 355–389.

Thilla, D. (2012). The economics of crime and punishment: an analysis of optimal penalty. Economics Letters 68 (2), 191–196.

Vanson, H. & Bourne, M. (2012) A social learning theory analysis of computer crime among college students. Journal of Research in Crime and Delinquency 34, 495–518.

Wiley,D. (2015) Towards cost-sensitive modeling for intrusion detection and response. Journal of Computer Security 10 (1–2), 5–22.

World Economic Forum (2012) Convergence on the outcome economy. Available at: http://reports.weforum.org/industrial-internet-of-things/3-convergence-on-the-outcome-economy/3-2-the-emergence-of-the outcomeeconomy/?doing_wp_cron=1463567483. 822540998458862304687 5

Yakubu, A.M (2019). The Effectiveness of Cybersecurity Compliance in a Corporate Organization in Nigeria. *International Journal on Recent and Innovation Trends in Computing and Communication,*Vol.7: 616 – 19.