Ehioghiren, Efe Efosa; Ojeaga, Joseph Oseikhuemhen; Eneh, Onyinye

Article

Cyber security : the perspective of accounting professionals in Nigeria

Provided in Cooperation with:
University of Benin, Benin City, Nigeria

Reference: Ehioghiren, Efe Efosa/Ojeaga, Joseph Oseikhuemhen et. al. (2021). Cyber security : the perspective of accounting professionals in Nigeria. In: Accounting and taxation review 5 (2), S. 15 - 29.
https://www.atreview.org/admin/12389900798187/Atreview%205(2)%2015-29.pdf.

This Version is available at:
http://hdl.handle.net/11159/6566

ISSN: 2635-2966 (Print), ISSN: 2635-2958 (Online).
©International Accounting and Taxation Research Group, Faculty of Management Sciences, University of Benin, Benin City, Nigeria.
Available online at http://www.atreview.org

Original Research Article

Cyber Security: The perspective of Accounting Professionals in Nigeria

Ehioghiren, Efe Efosa[1], Ojeaga, Joseph Oseikhuemhen[2] & Eneh, Onyinye[3]

[1] Department of Accountancy Shaka Polytechnic, Edo State, Nigeria

[2] Department of accounting, Faculty of Management Sciences, University of Benin, Benin City, Nigeria email: osejoeojeaga@yahoo.com

[3] Department of Accountancy, Nnamdi Azikiwe University, Awka. Email: o.eneh@unizik.edu.ng

For correspondence, email: ehioghiren2004@gmail.com

Received: 03/06/2021 Accepted: 30/06/2021

Abstract

*This study assesses cyber security, the perspective of accounting professionals in Nigeria***.** *Two objectives, as well as research questions and hypotheses, guided the study. The survey research design approach was used in the study. The population consists of 148 auditing firms in Edo State, and the sample size was 160 respondents. The hypotheses formulated were tested with F-test statistics using the Statistical Package for Social Sciences (SPSS) version 20.0 software package. The study reveals that there is high knowledge of accounting professionals in terms of cyber security and cybersecurity-related incidents from auditing firms in Nigeria as well as organisations disclosure of information regarding internal audit and controls on cyber security within the organisation in Nigeria firms The study concluded that despite the increasing attention cyber-security is getting in security politics, indeed, thinking about and planning for worst-case scenarios is a legitimate task of the national assemble legislation and recommended among other that all stakeholders should put their hand on the deck to ensure that more policy on cyber security framework are put on to protect, regulate activities in the cyberspace and firms should adopt cyber security as strategy to curb cybercrime-related activities as this will enhance the knowledge of accounting professionals in the selected areas of cyber security and further provide insights to policymakers and implementers to develop a cyber-security and cybersecurity-related incidents from auditing firms in Nigeria.*

Keywords: cyber security, accounting profession, information technology, cybercrime, accountants, accountability

Accounting & Taxation Review, Vol. 5, No. 2, June 2021

JEL Classification Codes: M41, M42, M49

Citation: Ehioghiren, E.E., Ojeaga, J.O., & Eneh, O. (2021). Cyber Security: The perspective of Accounting Professionals in Nigeria. *Accounting and Taxation Review, 5*(2): 15-29.

1. INTRODUCTION

The rapidly changing business environment and events in the world have created a demand for cyber security protection. The occurrence volume is increasing day by day, requiring filtered as per the victims and those waiting to be victims. The rise of transformative technologies such as sophisticated information technologies (IT), robotic processes, Blockchain, Artificial Intelligence (AI), automation & machine learning has undoubtedly raised concerns among many accountants. (Wallace, Lin, & Cefaratti (2011)

In todays' world, cyber security may conceivably be the most important challenge accountant's face. According to the AICPA, Cyber security has become a top concern for boards of directors and executives of many entities, regardless of their size or the industry in which they operate (AICPA 2017).

Turner (2018) added that the Internet has made the world smaller in many ways, but it has also opened us up to influences that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster. Seemma, Nandhini, and Sowamiya (2018) avow no clear-cut definition of security. However, security is a process, not an end state; it is the process of maintaining an acceptable level of perceived risk. Rosenzweig (2013) states that no organisation can be considered "secure" for any time beyond the last verification of adherence to its security policy. If your manager asks, "Are we secure?" you should answer, "Let me check." If they ask, "Will we be secure tomorrow?" you should answer, "I don't know." Such honesty will not be popular, but this mindset will produce more tremendous success for the organisation in the long run.

However, Rohrer and Hom (2017) affirm that cyber security is protected from cyber-attacks by internet-connected systems, including hardware, software, and data. They added that this security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security. McKenna (2017) agree that cyberspace is the environment in which communication over computer networks occurs as such almost everybody in one way or the other is connected to it for one reason or the others such as government, judiciary, lawmakers, militaries, police station, national security, banks, transportation sectors, health sectors, university, school and students. A high volume of activities occurs every minute, second, hours, daily, monthly, and yearly. Li, Peters, Richardson, and Watson (2012) suggested that attention should be given to the concept of cyber security by focusing on protecting computers, networks, programs and data from unintended or unauthorised access, change or destruction. Some people have ague that ICT is a single point of failure to businesses, while others see the advantages as more than the harms caused by cybercrime. Others believe in the principles of collective protection that "your security depends on mine and mine depends on yours", advocating that all users must come together and protect our cyberspace by creating and managing it from being vulnerable (Kahyaoglu & Caliyurt, 2018; Xu, Guo, Haislip, & Pinsker, 2019)

There are reports of hacking activities occurring all over the world, and Nigeria is not excluded. Islam, Farah, and Stafford (2018) agree that cyber security threats should be considered an enterprise risk management problem rather than classifying it as an information technology (IT) risk. It is vital to have an entity-level cyber security framework to communicate useful information and cyber security threats to stakeholders. O'Neill (2017) more is being done on cyber security in advanced countries than in developing countries. The American Institute of Certified Public Accountants (AICPA) has provided a framework as a component of a new System and Organization Control (SOC) for assurance engagements relating to cyber security. This cyber security report mainly focuses on three main areas of information; the management's description, the management's assertion and the practitioner's opinion. This framework aims to establish a common underlying language for cyber security risk management reporting guidelines that align with the US generally accepted accounting principles (AICPA, 2018a; AICPA, 2018b).

(Hugh, Anthony, Laura, and Mac (2018) further stated that accounting professionals are engaged and responsible for reporting and presenting statutory reports, and such professionals have very minimum guidance on reporting on cyber security and threats. Over the past years, cyber security has emerged as one of the significant risk challenges, and organisations that endure cyber-attacks tend to suffer from financial loss and severe reputational loss. Against this backdrop, this study is carried out to address these severe concerns of cyber security threats; this study intends to assess cyber security: the perspective of accounting professionals in Nigeria**.** Specifically, the questions buttressed in this study are to what extent accounting professionals' knowledge in terms of cyber security and cyber security-related incidents from auditing firms in Nigeria? How is organisations disclosure of information regarding internal audit and controls on cyber security within Nigerian firms?

2. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

Cyber Security

Cyber security is the process of safeguarding the programs, networks and systems of digital networks. It is often misinterpreted as information security or considered as IT security. IT security is considered to protect all information assets, which can be in a digital or hard copy format (Von Solms and van Niekerk, 2013; Yadav, 2017). Another critical aspect of cyber security structure is Information assurance (IA). It is the process of assuring information and managing risks related to the usage, processing, storage, and transmission of information or data and the systems and processes that use that information (Wang, Kannan, & Ulmer, 2013). Cyber security consists of technologies, processes, and controls designed to safeguard systems, networks, and technologies. Therefore, cyber security should not be considered in isolation rather a concept that encompasses information security and information assurance (Gyun No, & Vasarhelyi, 2017)

Why Do We Need Cyber Security?

The range of operations of cyber security involves protecting information and systems from major cyber threats (Gordon, Loeb, Lucyshyn, & Sohail, 2006). These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where cyber threats often take aim at secret, political and military assets of a nation, or its people in their most innovative form. Some of the common threats are as identified by (Haapamäki & Sihvonen, 2019):

i. Cyber terrorism is the innovative use of information technology by terrorist groups to further their political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.

ii. Cyberwarfare involves nation-states using information technology to go through something another nation's networks to cause damage. In the US and many other people who live in a society, cyber warfare has been acknowledged as the fifth domain of warfare. Cyberwarfare attacks are primarily executed by well-trained hackers who benefit from the quality of details computer networks and operate under the favourable and support of nation-states. Rather than closing a target's critical networks, a cyber-warfare attack may force to put into a situation into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.

iii. Cyber espionage: It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is often used to gain strategic, economic, military advantage and is conducted using cracking techniques and malware.

Who are Cyber Criminals?

It involves such activities as child printed sexual organs or activity; credit card fraud; cyber stalking; defaming another online; gaining unauthorised access to computer systems; ignoring copyright, software licensing and trademark safe to protect; overriding encryption to make illegal copies; software piracy and stealing another's identity to perform criminal acts (Banker & Feng, 2019). Cybercriminals are those who conduct such acts. They can be categorised into three groups that reflect their motivation.

Group 1: Cybercriminals – those hungry for recognition: Hobby hackers; IT professionals (social engineering is one of the most significant threats); Politically motivated hackers; and Terrorist organisations.

Group 2: Cybercriminals – those not interested in recognition: Psychological prevents; financially motivated hackers (corporate espionage); State-sponsored hacking (national espionage, sabotage); and organised criminals.

Group 3: Cybercriminals – the insiders: former employees seeking revenge; Competing companies using employees to gain economic advantage through damage and theft.

What Cyber Security Can Prevent

Cyber security can help prevent cyber-attacks, data breaches and identity theft and can help in risk management. When an organisation has a strong sense of network security and an effective incident response plan, it can prevent these attacks. For example, end-user protection defends information and guards against loss or theft while scanning computers for malicious code. (Curry, Marshall, Correia, & Crossler 2019)

Types of Cyber Security Threats:

The use of keeping up with new technologies, security trends, and threat intelligence is a challenging task. However, it should be to protect information and other assets from cyber threats, which take many forms. (Daniel & Julie, 2017)

i. Ransomware involves an attacker locking the victim's computer system files, typically through encryption and demanding a payment to decrypt and unlock them.

ii. Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.

iii. Social engineering is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

iv. Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

Computer vulnerabilities and threat agents

Growing dependence on web-based technologies and networks for their financial management systems has made private and public entities vulnerable to cyber-attacks (Gansler & Lucyshyn, 2005). Effective management is critical in an era of universal information, where the information travels through cyber space. To be an effective management, there should be increased awareness among the management team about cyber security vulnerabilities such as cyber-threats and information warfare. (Steinbart, Raschke, Gal, & Dilla, 2013). The terminology in information security is often seemingly congruent with the terminology in national security discourses: threats, agents, vulnerabilities, etc. However, the terms have precise meanings so that seemingly clear analogies must be used with care. One (of several possible) ways to categorise threats is to differentiate between 'failures', 'accidents', and 'attacks'. Failures are potentially damaging events caused by system deficiencies or an external element on which the system depends. Failures may be due to software design errors, hardware degradation, human errors, or corrupted data. Accidents include the entire range of randomly occurring and potentially damaging events such as natural disasters. Usually, accidents are externally generated events (i.e. from outside the system), whereas failures are internally generated events. Attacks (both passive and active) are potentially damaging events orchestrated by a human adversary (Seemma, Nandhini, & Sowmiya, 2018). They are the main focus of the cyber-security discourse. Human attackers are usually called 'threat agents'. The most common label bestowed upon them is a hacker. This catchphrase is used in two main ways, one positive and one pejorative (Chartered Global Management Accountant 2015). The computing community members describe a member of a distinct social group (or sub-culture); an exceptionally skilled programmer or technical expert who knows a programming interface well enough to write novel software (Burton, 2017). A particular ethic is ascribed to this subculture: a belief in sharing, openness, and free access to computers and information; decentralisation of government; and the improvement of the quality of life (Tanaka, Matsuura, & Sudoh, 2005). However, in popular usage and in the media, the term hacker generally describes computer intruders or criminals.

In the cyber-security debate, hacking is considered a modus operandi that can be used by technologically skilled individuals for minor misbehaviours and by organised actor groups with evil intent, such as terrorists or foreign states (Georg, 2015). Some hackers may have the skills to attack those parts of the information infrastructure considered 'critical' for the functioning of society. Though most hackers would be expected to lack the motivation to cause violence or severe economic or social harm because of their ethics (Diane & Tawei, 2019), government officials fear that individuals who can cause severe damage, but little motivation, could be corrupted by a group of malicious actors.

The need for a cyber security disclosure framework

Cyber security has emerged as a paramount risk issue for all types of organisations in the world. Therefore it is necessary for every organisation to at least consider the cyber security risk management program (Stevens, 2016). Further it is explicitly recommended to establish a cyber security disclosure framework; this would ensure that organisations can provide relevant, timely and useful information to the stakeholders about cyber security threats and the efforts taken by the organisations (AICPA, 2018a; AICPA, 2018b).

The American Institute of Certified Public Accountants (AICPA) provides the framework for an examination-level attestation engagement. This framework is a vital component of a new System and Organization Control (SOC) for cyber security engagement. This cyber security report provides information under the following three categories:

1) The management's description;
2) The management's assertion; and
3) The practitioner's opinion.

The ultimate aim of developing a framework for cyber security risk management and disclosure is to provide a consistent, market-based and relevant solution for the companies to communicate successfully with key stakeholders on how organisations have managed their cybersecurity-related risks (AICPA, 2018b). Listed entities should communicate to their investors about material risks and incidents promptly, including those companies that are subject to material attacks but may not have been a target of a cyber-attack. (Von & Van, 2013). Due to the increasing significance of cyber security incidents, SEC released its first guidance on cyber security in 2011. The SEC continues to consider other means of promoting appropriate disclosure of cyber security incidents and expanding the guidance issued in 2011 (Securities and Exchange Commission 2018).

Strategies for Dealing with Cyber security Risks

Thomson (2017) stated that a key or critical job requires lifelong learning, especially now in the rapidly changing age of digitalisation and related cyber security risks. He used the year 2007 as an example of such rapid change:

1) Apple released its first iPhone, starting the smartphone revolution that can provide anyone with an internet-connected computer.

2) Facebook opened itself to anyone with an email address and Twitter started to scale globally. 3) Amazon released Kindle which started the e-book revolution.

4) Google bought YouTube and introduced Android, an open-standards platform for devices that would help smartphones scale globally.

5) AT&T invested in software-enabled networks to expand its capacity to handle mobile cellular traffic which then increased more than 100,000% from 2007 through 2014.

6) IBM started Watson, the world's first cognitive computer, which combined machine learning and artificial intelligence.

7) Intel introduced non-silicon materials into its microchip transistors, extending the duration of Moore's Law, the expectation that the power of microchips would double about every two years, with the exponential growth in computer power still continuing to this day.

8) Internet users worldwide exceeded one billion which seemed to have been a tipping point for significant worldwide Internet use.

The role of professional accountant

The professional accountant has a lot to contribute to cyber security, as cyber security knowledge is needed in the professional practices with a robust institutional framework that will assist good corporate governance in the public and private firms that will build and install public confidence among the stakeholder and the entire business system (Gyun & Vasarhelyi, 2017). Gordon, Loeb, and Sohail (2010) added that this knowledge would also enhance the knowledge of accounting professionals in the selected areas of cyber security and further provide insights to policymakers and implementers to develop a cyber-security. Cheng and Walton (2019) avow that, most importantly, disclosure of information regarding internal audit and controls on cyber security within Nigerian firms will help provide litigation support service with appropriate provision of professional services in the law courts.

Castelluccio (2017) affirm that disclosing cyber security disclosures in the annual report provides an opportunity for the organisation to signal the markets that the organisation is actively engaged in preventing, detecting and correcting cybersecurity-related gaps. The professional association has key start bills on cyber security to be enacted to enable government and regulatory authorities to provide standards and guidelines to regulate cybercrimes activities. Above all, Nigerians should embrace integrity, objectivity, fairness, and accountability in their day-to-day activities.

There should be sensitisation of the course in our various higher schools of learning bring taught that will create the desire attention within the accounting lectures and the students. (Anis, 2017)

Investment in security technology is encouraged when imposed by regulations. Sarbanes-Oxley Act of 2002 (SOX) have strict regulations on the management and auditors to report on the effectiveness of the internal controls over the financial reporting component of the organisation's management information systems (Li et al. 2012). They added that accounting professionals must know internal controls and procedures about cyber security. Increasing cyber security incidents and reporting regulations require accounting professionals to know about cyber security. (Bain & Robinson, 2017). Therefore, accounting professionals need to possess knowledge of cyber security and cyber security-related incidents. Disclosing cyber security disclosures in the annual report provides an opportunity for the organisation to signal the markets that the organisation is actively engaged in preventing, detecting and correcting cybersecurity-related breaches. However, it is a strategic choice for organisations to decide whether or not to disclose items about cyber security incidents.

Lainhart (2000) suggested that the management requires adopting commonly applicable and accepted best IT governance and control practises as a benchmark for the prevailing IT environment. The level of technical expertise possessed by the internal auditors and the extent and quality of the internal audit report are positively correlated (Steinbart et al., 2013). Cyber security auditing is a new dimension of security practice intended to safeguard critical information assets (Islam, 2018). The cyber security auditing process will ensure the efficacy of organisational cyber security policies relating to safeguarding information integrity, information confidentiality, information accessibility and information availability (Haapamäki & Sihvonen, 2019). Internal auditors should expand their IT expertise and capabilities to provide proactive insights and value-added recommendations to the management (Kahyaoglu & Caliyurt, 2018). Wallace et al. (2011) suggested that the implementation of IT controls and the level of training given for the employees varies according to the size and nature of the organisation. Therefore organisations need to disclose information relating to internal audits and controls on cyber security. Cyber security has positively affected the share price (Gordon et al. 2010). Li et al. (2018) argued that SEC's disclosure guidance might unintentionally encourage organisations to disclose cyber security risks regardless of the magnitude of the risks. Therefore, it is essential for the organisation to disclose cyber security strategy.

Hypotheses

The following null hypotheses were formulated;

H_0: there is no knowledge of accounting professionals in terms of cyber security and cybersecurity-related incidents from auditing firms in Nigeria.

H_0: there is no organisations disclosure of information regarding internal audit and controls on cyber security within Nigerian firms

3. METHODOLOGY

Research Approach

This study follows a survey research design approach to assess the perspective of cyber security knowledge of the accounting professionals and disclosure of information regarding internal audits and controls on cyber security within Nigerian firms**.**

Population and sample

The population for the study consists of 148 auditing firms in Edo State, made up of managing partners, audit managers, tax managers, practitioner assistances, practitioner in-training financial accountants, management accountants, and internal auditors. In determining the sample size for the study, the researchers used the judgmental sample to pick (16) sixteen firms from Benin City. The total number of officers was 160; the researcher used the questionnaire to obtain primary data.

Questionnaire distribution

The questionnaire was designed in a structured form and were randomly distributed made up of general questions of two research questions groups as follows; section (A) five questions and section (B) seven questions to be measured via 5-point Likert scale according to the two hypotheses and was restricted with the responses made of Strongly agree (SA) agree (A) undecided (U) Strongly disagree (SD) and disagreed (D). Out of the 160 copies of questionnaires distributed, only 125 questionnaires were usable, representing a 78% overall response rate.

Data analysis technique

The 125 questionnaires were processed, and the hypotheses formulated for the study were tested with F-test statistics using the Statistical Package for Social Sciences (SPSS) version 20.0 software package.

Using SPSS, 5% is considered a normal significant level. F- test statistic was used to test the hypotheses formulated. The decision was that if F-value is equal or greater than the significant value, there is a significant interaction effect or significant difference, ie. F-value > significant value we reject Null and accept the alternative hypothesis.

4. ESTIMATION RESULTS AND DISCUSSION OF FINDINGS

Data Analysis and results

The data collected were analyses as show in the tables

Table 1: Knowledge of accounting professionals in terms of cyber security and cyber security related incidents

S/N	Statement	SA	A	U	D	SD
1	It is necessary for accounting professionals to possess knowledge of cyber security and cyber security related incidents	38	57	15	6	9
2	The intensity of desire and the perception of opportunity are personality variables to steal fluctuate cyber security and cyber security related incidents	49	42	5	22	7
3	The expectation of fair treatment and the fact that nobody	34	34	11	12	34

	likes to be duped has made cyber security and cyber security related incidents investigation grew in the society					
4	cyber security and cyber security-related incidents in Nigeria has not gained ore recognition as stakeholders are not aware of the relevance of the services rendered o the economy	70	45	2	5	3
5	professional standards do not require cyber security and cyber security related incidents to use professional scepticism, notwithstanding prior experience with the factors that increase the possibility of cybercrime management	85	21	6	3	10

Source: field survey, 2021

Table 2: Organisations disclosure of information regarding internal audit and controls on cyber security within Nigerian firms

S/N	Statement	SA	A	U	D	SD
6	cyber security is effective in designing internal control system for accounting practices that will lead to fraud detection and curbs fraudulent activities in Nigeria firms	9	10	8	51	47
7	It is necessary for organisation to disclose cyber security strategy and cyber security related incidents	61	37	7	13	7
8	Psychological factors influence the way a person interprets cybercrime and this, in turn, influence the action taking.	44	54	3	16	8
9	Cyber security system has improves stakeholder trust and confidence in the corporate financial statement.	6	8	2	76	33
10	Accountants/auditors with specialised knowledge and specific skills in cyber security will deliver more quality and high level of assurance services for fraud detection.	57	58	-	7	3
11	Cyber security regarding internal audit and controls of business environment identify weaknesses and areas susceptible to fraud or loss.	77	32	4	7	5
12	Organisation which suffers cyber-attack, have to face the losing assets, business reputation and potentially the organisation have to face regulatory fines.	66	37	2	9	11

Source: field survey, 2021

Validity and Reliability Tests

The cronbach's alpha was used to test the validity and reliability of the data which results was 0 .70 indicating that the data is valid, consistent and accepted for the study.

Test of hypotheses

Hypothesis one (null)

Ho: There is no knowledge of accounting professionals in terms of cyber security and cyber security-related incidents from auditing firms in Nigeria.

This hypothesis is tested with the data in table 1 using F- test statistics

Model Summary^{b}

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.928^{a}	.861	.814	1.735	2.800

a. Predictors: (Constant), U
b. Dependent Variable: KAPSC

Coefficients^{a}

Model		Unstandardised Coefficients		Standardised Coefficients	T	Sig.	95.0% Confidence Interval for B
		B	Std. Error	Beta			Lower Bound
1	(Constant)	122.669	1.234		99.368	.000	118.741
	U	.430	.100	.928	4.303	.023	.112

Source: field survey 2021 (Using SPSS)

An independent sample t-test was run with SPSS to determine if there were significant differences between predictor and KAPSC. The predictors were normally distributed according to the P-P plot, and homogeneity was slightly significant at 2.800. The response was most significant for U with t =4.303. The R- square at 0.861 shows that approximately 86% of the variance of KAPSC is accounted for by the model. Also, the F- value is statistically significant, meaning that there is high perception of knowledge of accounting professionals in terms of cyber security and cyber security-related incidents from auditing firms in Nigeria.

Hypothesis two (null)

Ho: No organisations disclose information regarding internal audit and controls on cyber security within Nigerian firms.

This hypothesis is tested with the data in table 2 and applying F- test statistics.

Model Summary^{b}

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.938^{a}	.879	.855	9.926	3.012

ANOVA^{a}

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	3588.267	1	3588.267	36.422	.002^{b}
	Residual	492.590	5	98.518		
	Total	4080.857	6			

Source: field survey 2021 (Using SPSS)
a. Dependent Variable: ODICS
b. Predictors: (Constant), U

The independent sample t-test was run with SPSS to determine if there were significant differences between ODICS and predictor. The predictors were normally distributed according to the P-P plot, and homogeneity was slightly violated at d = 3.012 meaning that the error is negatively correlated. The F-test, as well as t-test, are significant 2 0.002 and 21.932. The predicator U has the strongest correlation (positive) with ODICS. Therefore, the null hypothesis is rejected to accept the alternative that says that organisations disclose information regarding internal audit and controls on cyber security within Nigerian firms.

Discussion of Findings

The discussion is based on the findings of the two hypotheses for the study. Hypothesis one confirms that accounting professionals have high knowledge in terms of cyber security and cybersecurity-related incidents from auditing firms in Nigeria, as found in this study. This result is in agreement with the study carried out by Steinbart et al. (2013), who found that it is essential for accounting professionals to possess knowledge of cyber security and cybersecurity-related incidents.

Hypothesis two findings indicate that organisations disclose internal audit and cyber security controls within Nigerian firms. These findings concord with the study of Wang, Kannan and Ulmer (2013), who found the need for organisations to disclosed information regarding internal audit and controls on cyber security within the organisation.

5. CONCLUSION AND RECOMMENDATIONS

The research concludes that despite the increasing attention cyber-security is getting in security politics. Indeed, thinking about and planning for worst-case scenarios is a legitimate task of the national assembly legislation. However, in seeking a prudent policy, decision-makers difficulty is to navigate the rocky shoals between panic-stricken scenarios and uninformed satisfaction. Threat representation must remain well informed and well balanced not to allow overreactions with too high costs and uncertain benefits. As would most likely have hugely detrimental effects on the way humankind uses the Internet. Also, solving the attribution problem would come at a very high cost for privacy. Even though we must expect disturbances in the cyber-domain in the future, we must not expect outright disasters. Some of the cyber-disturbances may well turn into crises. Still, this crisis can also be seen as a turning point rather than an end state where the aversion of disaster or catastrophe is always possible. If societies become more fault-tolerant psychologically and more resilient overall, the likelihood for catastrophe in general and catastrophic system failure in particular can be substantially reduced. The way we imagine them influences our judgment of their likelihood, and there is an infinite number of ways in how we could imagine them.

It is recommended that all stakeholders put their hands on the deck to ensure that more policies on cyber security frameworks are put on to protect and regulate activities in cyberspace. Firms should adopt cyber security as a strategy to curb cybercrime-related activities as this will enhance the knowledge of accounting professionals in the selected areas of cyber security and further provide insights to policymakers and implementers to develop cyber-security and cybersecurity-related incidents from auditing firms in Nigeria.

It is further recommended that since organisations disclosed information regarding internal audits and controls on cyber-security within Nigerian firms, this should be sustained and encouraged as such disclosures will help provide litigation support service with appropriate provision of professional services in the law courts. Also, the disclosures in the annual report will help an opportunity for the organisation to signal the markets that the organisation is actively engaged in preventing, detecting, and correcting cybersecurity-related gaps

REFERENCES

American Institute of Certified Public Accountants (2017). SOC for Cybersecurity: Helping You Build Trust and Transparency. Durham, NC: AICPA.

American Institute of Certified Public Accountants (AICPA) (2018a). Cyber security risk management reporting fact sheet, available at: www.aicpa.org/content/dam/aicpa/

American Institute of Certified Public Accountants (AICPA (2018b). SOC for cybersecurity: a backgrounder, available at: www.aicpa.org/content/dam/aicpa/interestareas/frc/

Anis, A. (2017). Auditors' and accounting educators' perceptions of accounting education gaps and audit quality in Egypt. *Journal of Accounting in Emerging Economies*, 7 (3), 337–351.

Bain, B., & Robinson, M. (2017). Hackers May Have Profited From SEC Corporate Filing System Attack, bloomberg.com, September 20.

Buffett, W. (2016). "CEO Letters," Berkshire Hathaway Annual Reports.

Banker, R., & Feng, C. (2019). The impact of information security breach incidents on CIO turnover. *Journal of Information Systems, 33 (3), 309–329.* https://doi.org/10.2308/isys-52532

Burton, J. (2017). Cyberspace Aggression Adds to North Korea's Threat to Global Security, theconversation.com, August 15.

Castelluccio, M. (2017). My Robot's Staring At Me, Strategic Finance, March, 2017.

Castelluccio, M. (2017). The Most Notorious Hacks of 2016, Strategic Finance, January. CBS Mews (2017). Deloitte Hack Reportedly Hit Corporate, Government Clients, msn.com, September 25.

Chartered Global Management Accountant (2015). CGMA Cyber Security Risks Survey Data, CGMA, December 1.

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed? *Journal of Information Systems, 33 (3), 163–182. https://doi.org/10.2308/isys-52410*

Curry, M., Marshall, B., Correia, J., & Crossler, R. (2019). InfoSec process action model (IPAM): Targeting insider's weak password behavior. *Journal of Information Systems, 33 (3), 201–225. https://doi.org/10.2308/isys-52381*

Frank, M., Grenier, J., & Pyzoha, J. (2019). How prior cyberattacks influence the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of*

Information Systems, 33 (3),183–200. https://doi.org/10.2308/isys-52374

Daniel, S, & Julie, W. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12 (2), 56-68 ISSN 1558-7215.

Diane, J. J., & Tawei, W. (2019). Implications of cyber security on accounting information. *Journal of Information Systems American Accounting Association, 33, (3)23-31*

Gansler, J. S., & Lucyshyn, W. (2005). Improving the security of financial management systems: What are we to do?, *Journal of Accounting and Public Policy*, 24 (1), 1–9.

Georg L. (2015). Strategic Control: Pending Legal Responsibility of Non-Executive Boards for Governance in Information Security. EIASM Corporate Governance Workshop, October 25, 26.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25 (5), 503-530.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34 (3), 567-594.

Gyun No, W., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting*, 14(1), 1-12.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808–834.

Hugh, G., Anthony D. H., Laura, G. S., & Mac, C., (2018). Cyber security Guidance for Accountants and Executives. t: https://www.researchgate.net/publication/330199422

Islam, M. S., Farah, N., & Stafford, T. S. (2018). Factors associated with security/cybersecurity audit by internal audit function: an international study. *Managerial Auditing Journal*, 33 (4), 377-409.

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 33 (4), 360-376.

Li, C., Peters, G.F., Richardson, V. J., & Watson, M. (2012). The consequences of information technology control weaknesses on management information systems: the case of Sarbanes Oxley internal control reports", *MIS Quarterly*, 36 (1), 179-203.

McKenna, F. (2017). Equifax Auditors are on the Hook for Data Security Risk Controls, marketwatch.com, October 3.

O'Neill, E. (2017). Five Practical tips For Strong Cyber Security, Chartered Accountants Today, January 30. PriceWaterhouseCoopers (2015). Leading in Extraordinary Times, The 2015 US CEO Survey in CEOs' Words.

Rohrer, K. & Hom, N. (2017). Who's responsible for cybersecurity? *Strategic Finance, October* 1.

Rosenzweig, P. (2013). Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, The Great Courses. 25

Seemma, P.S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security.

International Journal of Advanced Research in Computer and Communication Engineering , 7 (11), 125- 128

Securities and Exchange Commission (SEC) (2018). Commission statement and guidance on public company cybersecurity disclosures, available at: www.sec.gov/rules/interp/2018/33-10459.

Stevens, T. (2016) Global Cyber security: New directions in theory and methods. *Journal* of *Politics and Governance. 6 (2). doi:10.17645 /pag.v6i2.1569.*

Steinbart, P. J., Raschke, R., Gal, G. F., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions, Journal *of Information Systems*, 27 (2), 65-86.

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: an empirical analysis of E-local government in Japan, *Journal of Accounting and Public Policy*, 24 (1), 37-59.

Thomson, R. (2017). Schumer Compares Equifax to Enron: Disgusting, Deeply Troubling, newsmax.com, September 14.

Traina, L. (2015). The top 5 Cyber-security Risks for CPAs, cpa2biz.com, June 15.

Turner, R. (2018). Thinking about cyber-attacks in generations can help focus enterprise security plans. Informa PLC. Ovum.

Von, S., R., & Van N., J. (2013). From information security to cyber security, *Computers and Security, 38, (1), 97-102.*

Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information security and sarbanes-oxley compliance: an exploratory study. *Journal of Information Systems*, 25 (1), 185-211.

Wang, Y., Kannan, K. & Ulmer, J. (2013). The association between the disclosure and the realisation of information security risk factors. *Information Systems Research*, 24(2), 201-218.

Xu, H., Guo, S., Haislip, J. Z., & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems 33 (3), 267–284.* *https://doi.org/10.2308/isys-52480*

Yadav, A. (2017), Cyber Security, Alpha Science International Lt, Oxford.