INTERNAL FACTORS INFLUENCING CYBER SECURITY COMPLIANCE AMONG CIVIL SERVANTS IN AWKA SOUTH LGA

Chikwendu, Stephen Chilaka
Department of Sociology and Anthropology,
Nnamdi Azikiwe University, Awka, Anambra State, Nigeria
Email: sc.chikwendu@unizik.edu.ng

Obiefuna, Nneka Marina
Department of Sociology and Anthropology,
Nnamdi Azikiwe University, Awka, Anambra State, Nigeria
Email: nm.metala@unizik.edu.ng

Anaekwe, Henry Ebuka
Department of Sociology and Anthropology,
Nnamdi Azikiwe University, Awka, Anambra State, Nigeria
Email: he.anaekwe@unizik.edu.ng

Abstract
This study investigated internal factors influencing cyber security compliance among civil servants in Awka South LGA. Reinforcement theory by B.F. Skinner was adopted as the theoretical framework of the study. The mixed methods research design was adopted for the study. The multi-stage sampling procedure which was made up of cluster and simple random sampling procedure was used in selecting a sample size of 204 respondents for the study. The quantitative data were analyzed using descriptive statistics such as the frequency counts and simple percentages while the qualitative data were analyzed using the thematic method of data analysis.. Findings showed that internal factors influencing cyber security compliance among civil servants include management policy on cyber security, computer literacy level, work ethics and improved supervision of workers. Consequences of non-compliance to cyber security among civil Servants in Awka South LGA include data loss, bad public image, low productivity, security breaches and cyber attacks. The study therefore recommends amongst others the need for awareness creation on the benefits of cyber security compliance in Awka South LGA. Also, there is need for periodic update of office software and operating systems for civil servants in the study area.

Introduction

The global trends in cyber security concerns occur because many workers do not adequately comply with the available cyber security safety regulations in the workplace (Ahmed, Kulsum & Bin, 2017). Employees, especially civil servants represent a significant security vulnerability that exposes organizational assets to external and internal cyber attackers. It has been observed that humans are the weakest link. The human factor is the most common way through which hackers get unauthorised access to vital systems in a protected environment (Bergstrom, Lundgren & Ericson, 2019). In this age of internet evolution and digital systems, cyber security stands as a very important subject for every individual, organization and government that seeks to operate efficiently and under minimal risk (Carder, 2018; Fasilat & Satirenjit, 2021). Also, Gana, Abdulhamid and Ojeniyi (2019), pointed out that Information and Communication Technology (ICT) has impacted significantly on institutional operations, processes and products such that cyber security now stands a necessity for every organization. Cyber security however, is not merely a function of employing a few tools and personnel that would manage the ICT systems; it is rather a culture that should be interwoven into the fabrics of all organizational processes of concerned organizations and institutions.

According to Girma and Lemma (2020), just as ICT have gradually crept into our daily lives, organizations, government and every citizen has been inducted into the cyber world one way or the other. Hence, just as security is a necessity in the physical world, it has also become a necessity in the cyber world. In this sense, compliance to cyber security becomes necessary because employees and organizations are faced with safety and security challenges every time they go online. For this reason, Madu (2020), asserted that the need for cyber security compliance among civil servants is undisputed, as it remains the first factor or line of defence in providing civil servants with the technical know–how to interact on the internet safely.

There are a number of factors influencing cyber security compliance among civil servants in Nigeria. These factors can be categorized into internal factors and external factors (Alkalbani, Olusola, Alaba, Ogunleye & Adebiyi, 2020). The internal factors influencing cyber security compliance among civil servants are as follows: computer literacy, existence of office safety protocols, training and capacity building, safety manuals, punishment for non-

compliance to cyber security practices, reward for compliance amongst others. Similarly, external factors promoting cyber security compliance among civil servants include: proliferation of cyber attacks on government institutions, high rate of identity theft, corporate data loss, the need to improve service delivery, data protection, awareness of the consequences of non-compliance to cyber security, extant law ensuring compliance, etc. (Alkalbani, Olusola, Alaba, Ogunleye & Adebiyi, 2020). With increasing number of cyber-attacks, organizations can face serious losses and need to consider investing in cyber security practices. This explains why some organizations are beginning to adopt a wide range of technical and procedural approaches to secure data and information through encryption and security awareness campaigns (Chikwendu & Oli, 2023).

In Nigeria, it has been observed that cyber security compliance among civil servants is low (Ugbe, 2021). Odey and Onebieni (2021) observed that some civil servants wrongly believe that cyber security is the responsibility of the government and in-built security applications or tools like antivirus and firewalls. Some civil servants have argued that cyber security should be handled by the Information Technology (IT) department of their workplaces; this situation has made many civil servants not to comply with basic cyber safety measures. According to Maisikeli (2020), the human factor has been the weakest link through which many successful cyber attacks have been perpetuated. Yet many civil servants are not fully aware of their roles towards ensuring cyber security in their organization. Another situation that suggests setback to cyber security among civil servants is the belief that even though cyber threat is real, they can never become victims. These set of employees feel that sensitive institutions such as banks should be more concerned about cyber security. Madu (2020) posits that out of sheer ignorance some civil servants in Nigeria think that they are well secured by their optional and sometimes limited cyber security practices. There are also civil servants who do not see cyber threat as a big deal to be prioritized simply because it does not inflict physical harm (Kostyuk & Wayne, 2019; Fasilat & Satirenjit, 2021).

As widely reported in the media, cyber attacks are increasing in quantity and sophistication (Gilheany, 2017; Odey & Onebieni, 2021). In most cases, it is the weakest link in cyber security (i.e. the human element) that is being targeted by hackers. Unfortunately, a large number of civil servants in Nigeria are lacking in cyber security compliance and this problem has wider implications on personal, organizational data and confidential documents. This low cyber security compliance rate manifests in daily activities of many civil servants. In the light of the above, Chai (2021) observed that there are some civil servants who are unaware of the existence of agencies responsible for handling issues of cyber security breaches in the country, let alone the knowledge of the 2015 Cyber Security Act. A Study by Odey and Onebieni (2021) concentrated on cyber security risks such as malware-infected websites and theft of personal data in Nigeria and revealed that there is poor understanding and limited compliance to cyber security updates among civil servants. It follows therefore that cyber security compliance among civil servants is abysmally poor and many workers are not aware of how to protect office data, thereby exposing them to possible cyber attacks and data loss.

For Maisikeli (2020), lack of cyber security compliance can lead to any of the following consequences: data loss, low productivity, bad reputation, law suits, etc. Inadequate end-user security, employee negligence and weak password management are some of the reasons why hackers sometimes succeed in infiltrating computer systems. Once cyber attacker breaches organization's network, data can be stolen or corrupted. Loss of data integrity is disastrous if an organization does not have a backup plan. Data theft or loss has grounded and led to the closure of many businesses and organizations today. Kostyuk and Wayne (2019) buttressed that downtime caused by cyber attacks may lead to decline in productivity. When systems become infected with malware (i.e. computer virus), employees cannot perform routine tasks while the issue is remediated and systems restored. Unplanned downtime negatively impacts the organization, affects service delivery, revenue and promotes poor attitude to work.

Cyber security compliance should be everybody's concern the same way that security in the physical space is everybody's business. Previous studies have identified factors such as computer literacy skills, data safety and protection as influencing cyber security compliance in Nigeria (Ahmed, Kulsum & Bin, 2017; Alkalbani, Olusola, Alaba, Ogunleye & Adebiyi, 2020; Odey & Onebieni, 2021). Apart from the fact that these previous studies relied mainly on secondary sources of data collection, none focused exclusively on internal factors influencing cyber security compliance among civil servants in Awka South LGA. This research addresses two question. The first is to identify the internal factors influencing cyber security compliance among civil servants in Awka South LGA of Anambra State while the second is to identify the consequences of non-compliance to cyber security among civil servants in Awka South LGA

Related Literature

Understanding Cyber Security

The term 'cyber' refers to features or characteristics relating to the culture of computers, information technology and virtual reality (Girma & Lemma, 2020). Thus, cyber security is the application of technologies, processes and controls to protect systems, networks, programmes, devices and data from cyber attacks (Girma & Lemma, 2020). According to Huyghue (2021), cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. It is also known as information technology security or electronic security. The term cyber security applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories such as network security, application security, informational security, operational security, disaster recovery and business continuity and end-user education.

Chai (2021) opined that recent advances in technology and the proliferation of digital technologies like cloud computing, mobile and personal computing devices has enabled a lot of global crimes to be committed in the cyber space. Consequently, it has become imperative that cyber security compliance mechanisms become integrated into the fabrics of everyday use of computer. Therefore, cyber security is the practice of protecting systems, networks and programmes from digital attacks. It also refers to any activity carried out to ensure integrity, confidentiality and availability of information systems. The global cyber security threat continues to evolve at a rapid pace, with a rising number of data breaches each year. Chai (2021) reported that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone across the world. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Alkalbani, Olusola, Alaba, Ogunleye and Adebiyi (2020) noted that medical services, retailers and public entities often experience the most breaches, with malicious criminals responsible for most incidents. Some of public sectors in Nigeria are more appealing to cyber criminals because they collect financial and medical data. However, all businesses that use networks can be targeted for customer data, corporate espionage or customer attacks. As posited by Fasilat and Satirenjit (2021), with the scale of cyber security threats set to continue to rise, global spending on cyber security solutions is naturally increasing. In the same vein, Fasilat and Satirenjit (2021) predicted that cyber security spending will reach $188.3 billion in 2023 and surpass $260 billion globally by 2026. This calls for urgent action by stakeholders before the situation (i.e., cyber security threat) gets out of hand.

Who are Civil Servants?

Ferreira and Serpa (2019) conceived civil servants as professionals who work for the government at the local or federal level. Civil servants work to benefit the general public every day. As civil servants, salaries, benefits and career advancement opportunities often vary significantly depending on job roles and requirements. Ahmed, Kulsum and Bin (2017) defined the term civil servants as a wide variety of employees and careers that serve as the engine room of the government. There are many convincing reasons why someone might want to seek a career in civil service. First, working for the government provides an attractive level of job security. Most of the services that civil servants provide ensure the protection of human rights and rule of law, stipulated and guaranteed by the government such as safety, justice and education. According to Amuta (2020), the benefits of civil service will vary by position, but most government employers are seeking to retain skilled employees and will offer competitive packages. The salaries of civil servants typically increase regularly according to how many years an employee has worked.

According to Antunes, Maximiano, Gomes and Pinto (2021), civil servant jobs are diverse. Common examples of civil service jobs include teachers, armed forces, judges, engineers, social workers, police officers among others. Teachers who teach in public schools are considered civil servants. Their salaries are paid by taxpayers, and they serve the public sector by educating children. The armed forces are responsible for protecting Nigeria and its citizens. Military civil servants include members of the Navy, Air Force, Army and many more. The armed forces offer a wide range of job titles including soldiers, pilots, engineers, officers, doctors, nurses, IT technicians, translators, mechanics and lawyers. Employees of the armed forces must all pass an entrance exam and must take an aptitude test that places them in a certain military branch or role. Similarly, the judicial branch of the government provides some interesting job opportunities, one of which is to serve as judge. Judges work in state and federal courtrooms, presiding over legal trials.

Gana, Abdulhamid and Ojeniyi (2019) added that another form of civil service is a civil engineer. Civil engineers build and maintain public roadways, bridges and railways. Some specialize in working with sewage systems, water treatments or dams. Types of civil engineers include electrical engineers, mechanical engineers, health and safety engineers. Police officers are another set of civil servants that protect the public and keep the peace by apprehending criminals. They investigate crimes, take criminals into custody and testify in criminal trials. Police officers are frequently the first to respond to emergency calls. One important set of civil servants are known as

social workers. Gana et al (2019) maintained that social workers help individuals handle issues like gambling and drug addiction, child abuse, loss of housing, unemployment and health problems. Public health social workers are professionals who provide support to those suffering from illness or substance abuse. In addition to these specialized jobs, it is also possible to hold a typical job title but serve in a civil capacity. For example, one can be a professional assistant or accountant for a local government, security guard etc. No matter what your job description may be, if one works for the Nigerian government, such a person is considered a civil servant.

Internal Factors Influencing Cyber Security Compliance among Civil Servants

In this current digital era, it is increasingly difficult to preserve the confidentiality, integrity and availability of an organization's information and technology assets against cyber attacks (Gilheany, 2017). Organizations and government agencies cannot rely solely on technical solutions for data protection and defence, since many cyber attacks attempt to exploit non-technical vulnerabilities such as how well civil servants (i.e., employees) comply with the organization's cyber security policies and practices. Many scholars have explored the internal factors that influence compliance to cyber security policies. Scholars such as Ghosemajumder (2017) revealed that understanding employee intentions towards compliance with information security is an important step in determining the internal factors that promote cyber security compliance. Kostyuk and Wayne (2019) identified several of these internal factors, one of which is related to social and work environment. Another internal factor is linked to the management and administration's approach to cyber security awareness among its employees and the cyber literacy level or culture of these employees (i.e., civil servants).

Maisikeli (2020) argued that lack of better strategy for cyber security that would provide strong data protection appears to be one of the internal factors that promote cyber security compliance among employees. In other words, fear of losing vital data or piece of information has forced many employees to learn basic ways to protect their data at work. Other internal factors influencing cyber security compliance among civil servants include: end user awareness, policy control measures, accountability, monitoring, organizational rules, regulations, ethics and commitment. This also means that technical security measures are promoting cyber security compliance among civil servants in Nigeria. It is for this reason that Ugbe (2021) opined that ethical factors have the most influence on civil servants compliance to cyber security policies, followed in decreasing order of influence by legislative factors, technical factors and administrative factors. In the current digital era, it appears to be difficult to preserve the confidentiality, integrity and availability of an organization's information and technology assets against cyber attacks. This is why organizations cannot rely solely on technical solutions for defence, since many cyber attacks attempt to exploit non-technical vulnerabilities such as how well employees comply with the organization's cyber security policies or guidelines.

Effiong (2021) carried out a study titled: Nigeria becomes world's second highest producer of cybercrime behind US. The study was conceived to identify internal factors influencing cyber security compliance among civil servants in Uyo metropolis, Akwa Ibom State, Nigeria. The study disproportionately sampled 255 men and women aged 18 years and above. The findings showed amongst others that majority (85.0%) of the respondents are aware of the factors influencing cyber security compliance among civil servants in Uyo, 10.0% were not aware while 5.0% of the respondents were indifferent. Further findings showed that internal factors influencing cyber security compliance among civil servants include: the fear of data loss, organizational rules and regulations and improved supervision of government employees. It was observed that cyber security threat is a common phenomenon in Uyo and as such organizations and government agencies are always on high alert in order not to become victims of cyber attacks. The study concluded that cyber security is a necessity in all the state agencies in Uyo State because it remains the first factor and line of defence in providing civil servants with the technical know–how to interact on the internet safely.

Similarly, Madu (2020) examined Nigeria's lead in Africa's cybercrimes. The study was carried out in Port Harcourt City in Rivers State. The motivation behind the study was to identify specific remote reasons that encourage cyber security compliance among civil servants. Using a sample size of 300 respondents comprising male and female State and Federal government employees working in Port Harcourt Rivers State between the ages of 18 and 60, it was found that there are various internal factors influencing cyber security compliance among civil servants in Port Harcourt, Rivers State, Nigeria. These factors in no particular order include: computer literacy, existence of office safety protocols, training and capacity building, safety manuals, punishment for non-compliance to cyber security practices, reward for compliance amongst others. The study hypotheses were tested using the *P–value of 0.05* and results established that civil servants with higher levels of education are likely to comply to cyber security safety tips more than their counterparts with lower levels of education. The second hypothesis was tested using correlation statistics and findings revealed that statistical relationship exist between age and compliance to cyber security among civil servants. This means that younger civil servants are likely to comply to cyber security safety whereas older civil servants are less likely to observe cyber security compliance.

Consequences associated with Non-compliance to Cyber Security among Civil Servants

Information is the critical resource of today's civil service operations and management. As a result, organizations often establish information systems to manage their information resources. These systems are interconnected internally, externally and globally so as to quickly process and share information to potential users. However, this interconnection exposes organizations to different information security threats. Information security threats occur during storage, processing, publication and dissemination (Chandarman & Van-Niekerk, 2017). Amuta (2020) argued that most of the information security threats come from employees unintentional and intentional actions. Empirical evidence shows that more than 70 percent of security threats come from insiders rather than from external agents. This problem is usually associated with lack of knowledge about information management and security policy implementation in the organization. As a result, employees are not aware about the consequences and damages of violating information security policy and procedures.

Bergstrom, Lundgren and Ericson (2019) reported that there are many consequences associated with non-compliance to cyber security among civil servants. These consequences include loss of data, cyber attacks, spamming and cyber security breaches have been linked to human factors also known as human errors. According to Chai (2021), threats and risks related to cyber security have increased significantly, thereby effectively becoming a serious burden to organizations and entities. Particularly exposed are organizations whose cyber security vulnerabilities are attracting increased attention. The reasons for an organization's security vulnerabilities are numerous. Employees, not systems, are the main targets of cyber attackers, and so, in actual sense, human failures manifesting through non-compliance to cyber security updates are to blame for most cyber attacks in organizations and government agencies in Nigeria. Therefore, cyber security policies for civil servants should be re-examined in Nigeria. As indicated by Alkalbani, Olusola, Alaba, Ogunleye and Adebiyi (2020), when organizations fail to prevent security breaches due to non-compliance among its staff it leads to consequences such as data loss, loss of sponsors and revenue, bad publicity, lawlessness and low productivity.

Fasilat and Satirenjit (2021) noted that the global trends in cyber security concerns occur because many workers do not adequately comply with the available cyber security safety regulations in the workplace. Employees, especially civil servants represent a significant security vulnerability that exposes organizational assets to external and internal cyber attackers. It has been observed that humans are the weakest link. The human factor is the most common way through which hackers get unauthorised access to vital systems in a protected environment. In this age of internet evolution and digital systems, cyber security stands out as a very important subject for every individual, organization and government that seeks to operate efficiently and under minimal risk. It is therefore not surprising that Gana, Abdulhamid and Ojeniyi (2019) observed that Information and Communication Technology (ICT) has impacted significantly on institutional operations, processes and products such that cyber security now stands a necessity for every organization. Cyber security however, is not merely a function of employing a few tools and personnel that would manage the ICT systems; it is rather a culture that should be interwoven into the fabrics of all organizational processes of concerned organizations and institutions to prevent consequences such as cyber attacks and security breaches.

Yusuf and Ahmed (2020) investigated the problems associated with non-compliance to cyber security among civil servants in six area councils of the F.C.T. (Federal Capital Territory), Abuja namely: Abaji, Gwagwalada, Bwari, Kuje, Kwali and Abuja Municipal. In a nutshell, the study was aimed at identifying the consequences associated with failure of staff to comply with safety guidelines in the use of the internet. The study adopted the concurrent mixed methods research design and used multistage sampling procedure to select 240 respondents consisting of males and females of the public. Results showed that majority (70.0%) of the respondents indicated that one of the major consequences associated with non-compliance to cyber security among civil servants is data loss and data theft. Others include loss of job and hardship (20.0%) and loss of revenue to the organization thereby affecting the public image and revenue target of the organization. The study observed that when a breadwinner is fired for negligence of duty (non-compliance to cyber security), his family and other dependants will suffer hunger, poor health, complications and death in extreme situations.

Amuta (2020) carried out a similar study to examine the consequences of non-compliance to cyber security among civil servants in Warri, Delta State. The study used a descriptive survey method and simple random sampling technique to select a total of 300 civil servants consisting of 150 men and 150 women. Instruments for data collection were questionnaire and Focus Group Discussion (FGD). The quantitative data (i.e., structured questionnaire) were analyzed using descriptive statistics whereas the qualitative data were analyzed using content method of data analysis. Findings showed amongst others that there is a positive relationship between non-compliance to cyber security and data loss in the civil service in Warri. 60.0% of the respondents indicated that non-compliance to cyber security safety tips often leads to avoidable consequences such as identity theft, cyber

attacks, data loss and low productivity. In the same vein, 40.0% of the respondents indicated that non-compliance to cyber security affect employees' attitude to work and may lead to work rivalry and poor service delivery.

Theoretical Framework

The theoretical framework adopted for this study is the reinforcement theory by B.F. Skinner. . This theory was proposed by B.F. Skinner (1904-1990) and his associates. Reinforcement theory stressed that behaviour is the function of its consequence. The theory rightly assumes that behaviour is usually driven by the social environment. This means that what controls behaviour are not internal cognitive events but "reinforcements" that is, any action or consequence that is rewarded or demonstrated following a response increases the probability that the behaviour will be repeated (Robbins, 2001; Nnonyelu, 2009). Reinforcement theory is not about what initiates behaviour but what happens when an individual's takes action. It is based on the law of effect and concept, which entails that an individual is likely to repeat certain actions or feelings if they have positive consequences and will avoid those behaviours that result in negative or unpleasant outcomes.

The reinforcement theory provides explanation as to why civil servants may desire to adhere to cyber security for data integrity and growth of their organizations. This means that the propensity to stick to cyber security safety tips is reinforced by the operational benefits and the satisfaction derived from it. Hence, Maisikeli (2020) discovered in their study that there are some levels of dissatisfaction in the policy guidelines concerning data management in the civil service in developing countries such as Nigeria. This dissatisfaction impairs tendency towards cyber security compliance and leads to several consequences such as data theft and loss of revenue. It has been observed that delays in adhering to safety rules and negligence are some of the human factors that cyber attackers exploit to steal data. Thus, the operational system in an organization either inspires or dampens the morale of civil servants to comply with cyber security guidelines. The reinforcement theory therefore emphasizes the need to adopt the best strategy that will encourage civil servants to imbibe data protection ethics and to promote the culture of cyber security compliance in the society.

This theory has been criticised on the ground that much of the current reinforcement theory in the operant tradition is more concerned with understanding the motivational features of reinforcement rather than predicting the effect on the distribution of available activities. Neo-behavioural theories that relate reinforcement to motivation have argued that even with adequate awareness and potential benefits of reinforcement or reward on the use of cyber security, there will always be workers who prefer the manual and old ways of doing things, which makes the assumptions of reinforcement theory limited and unilinear.

Methods

Design

This study adopted mixed methods research design because it is a research tool that makes use of quantitative and qualitative methods of data collection to gather information simultaneously. The essence of the mixed methods research design was to gain a deeper knowledge into the issue of discourse and to achieve a high level of certainty. It is instructive to note that by integrating both quantitative and qualitative data, the researcher gained both depth and breadth. Therefore, by leveraging on the advantages of the quantitative and qualitative methods, this approach balanced the downsides of each. The quantitative instrument was used to collect data through questionnaire while the qualitative component elicited information through in-depth interview (IDI) collected from a few research participants.

Study Area

This study was carried out in Awka South LGA, Anambra State. Anambra State was created on 27th August, 1991. Anambra was part of the former Eastern region, part of the former East Central State, and part of the old Anambra State. It is one of the thirty-six states of the Federal Republic of Nigeria and one of the five states of the Southeast geo-political zone. It shares boundaries with Delta State to the west, Imo State to the south, Enugu State to the east and Kogi State to the north. The state drives its name from Omambala River, the largest, most southerly, leftbank tributary of the River Niger. Anambra is the Anglicized name of the Omambala. With a total land area of 4,416 square kilometres, Anambra State situates on a low elevation on the eastern side of the River Niger (Anambra State Government, 2020).

In a related development, Awka South LGA is the capital of Anambra State and is located about 600 kilometres east of Lagos in the centre of the densely populated Igbo heart land in South Eastern Nigeria (Awka History & Facts, 2021). In the past, the people of Awka South were well known for blacksmithing, metal working and were respected for making farm implements, guns and tools. Awka South in earlier time was the site of Nri Civilization that produced the earliest documented bronze works in sub-Saharan Africa around 800AD. Today, they are respected among the Igbo people of Nigeria for their technical and business skill. Before the inception of the

British rule, Awka South was governed by titled men known as Ozo and Ndilchie who were accomplished individuals in the community and held general meetings either at the residence of the oldest man (Oto Chalu Awka) or at a place designated by him. Awka South is made up of nine towns, namely, Amawbia, Awka, Ezinato, Isiagu, Mbaukwu, Nibo, Nise, Okpuno and Umuawulu. There are three major streets that span this area, which are the Zik Avenue, Works Road and Arthur Eze Avenue.

Anambra civil service employees are made up of 18 ministries and 11 non-ministries departments. In addition, there are 7 other bodies outside the state civil service with civil servants posted to them. Civil service employees in Anambra State under periodic screening and competence test before they are promoted. There were claims that civil servants in Awka South LGA were lagging behind in terms of cyber security compliance. This assumption prompted the present researcher to embark on this study with a view to identify internal and external factors influencing cyber security compliance among civil servants in Awka South LGA and to chart a way forward.

Population of the Study

Published survey by Chukwurah, Daniel, Uzor, Iwuno, Chukwueloka and Chioma (2020) revealed that the staff strength of civil servants in Anambra State is 5,327. The breakdown showed that there were 2,125 males and 3,202 females. The targeted population for this study were civil servants aged 18 years and above working in Anambra State. Employees aged 18 years and above were chosen for this study because they have reached the age of consent and presumed to be familiar with the subject of this inquiry.

Sampling

A sample size of 204 respondents was adopted for the quantitative component of this study. Taro Yamane's statistical formula (1967) was used to determine the sample size as follows. The formula was given as thus, n = $\frac{N}{1+N\ (e)^2}$

Where: n = sample size, N = population of the study, 1 = constant, e = level of precision

Thus,

$n = \frac{5,327}{1+ 5,327\ (0.07)^2}$

$n= \frac{5,327}{1+ 5,327(0.0049)}$

$n= \frac{5,327}{5,328\ (0.0049)}$

$n = \frac{5,327}{26.1072}$

n = 204.0433

n= 204 (approximately). This figure was rounded up to two hundred and four (204) as the sample size for this study. The sample size was considered appropriate and adequate enough for statistical coding and analysis of the phenomenon under study. This sample size was believed to be true representation of the larger population because it is done in such a way that every element of the population had equal chance of being selected.

Data Collection and Analysis

Data was collected using questionnaire and IDI guides. The quantitative data were processed with the help of Statistical Package for Social Sciences (SPSS) version 24. The data were analysed with descriptive statistics such as frequency distribution tables, percentages and graphic illustrations which included bar charts and pie charts to present the characteristics of the research subjects. The Chi-square (x^2) statistical tool was used to test the stated hypotheses. In analysing the qualitative data, the researcher commenced with careful coding and transcribing of the raw data. The transcripts derived from the in-depth interviews were thoroughly read and coded. However, illustrative quotes, expressions, ideas and coded ideas were identified and organized under distinct themes. Manual thematic method was used in the analysis of the qualitative data. These qualitative data were compared with the quantitative data to establish a synergy between the two findings.

Findings

Table 1: Personal data of respondents

Variable	Frequency	Percentage
Sex		
Male	61	31.0
Female	139	69.0
Total	200	100
Age		
18-27	25	4.3
28-37	41	48.3

38-47	21	16.7
47 and above	30	22.8
Total	200	100
Marital status		
Single	61	30.2
Married	107	57.2
Divorce	11	11.2
Widowed	24	12.2
Separated		
Total	200	100
Religious affiliation		
African Traditional Religion	35	21.8
Islam	5	9.6
Atheist	10	15.8
Christianity	150	65.8
Total	200	100
Occupation		
Civil servant	16	3.2
Business	66	31.6
Farming	38	21.7
Unemployed	62	30.9
Total	200	100
Place of Residence		
Awka Urban	152	77.2
Awka Rural	48	33.8
Income Status	200	100
Low Income Earner	107	45.2
Average income Earner	67	23.1
High Income Earner	41	13.9
Total	200	100
Educational Qualification		
FLSC	25	13.1
SSCE	47	26.2
Diploma/OND	53	31.2
HND/B.SC	65	46.1
Higher degree	15	5.2
Total	200	100

Field Survey, 2025

Table 1 shows that majority of the respondents (69.0%) are females. The table also shows that majority of the respondents (48.3%) are between the ages of 28-37. On the marital status of the respondents, table 1 shows that majority of them (57.2%) are married. Further findings show that majority of the respondents (65.8%) opined that they are Christians. Also, the table shows that majority of the respondents (31.6) are into business. On place of residence, majority of the respondents (77.2%) indicated that they reside in the urban part of Awka, finally as regards educational qualification, (45.2%) indicated that they are low income earners, (46.1%) of the respondents posited that they only have HND/B.Sc.

Question One: What are the internal factors influencing cyber security compliance among civil servants in Awka South LGA?. Findings are presented in Table 2.

Table 2: Respondents' views on the internal factors influencing cyber security compliance among civil servants in Awka South LGA

Responses	***Frequency***	***Percentage***
Management policy on cyber security	27	12.1
Computer literacy level	54	32.1
Work ethics	45	24.1
Improved supervision of workers	37	17.2
All of the above	123	42.4
Total	200	100

Field Survey, 2025

Table 2 shows that majority of the respondents (42.4%) indicated that all of the following which include; management policy on cyber security, computer literacy level, work ethics, improved supervision of workers are the internal factors influencing cyber security compliance among civil servants in Awka South LGA. This aligns with data from the interviews conducted.

One of the interviewees stated:
There are a lot of internal factors influencing cyber security compliance among civil servants in Awka South Awka. These factors in no particular order include: computer literacy, existence of office safety protocols, training and capacity building, safety manuals, punishment for non-compliance to cyber security practices, reward for compliance amongst others (Female, 32, Civil Servant, Married, Awka Urban).

Underscoring the above stated fact, another interviewee stated:
To me, the internal factors influencing cyber security compliance among civil servants in Awka South Awka are the fear of data loss, organizational rules and regulations and improved supervision of government employees (Male, 35, Artisan, Awka Rural).

Objective Two: What are the consequences of non-compliance to cyber security among civil servants in Awka South LGA? . Findings are presented in table 3.

Table 3: Respondents' views on the major consequences of non-compliance to cyber security among civil servants in Awka South

Responses	***Frequency***	***Percentage***
Data loss	45	35.1
Bad public image	30	22.1
Low productivity	36	24.8
Security breaches	49	37.2
Cyber attacks	69	45.3
Total	200	100

Field Survey, 2025

Table 3 shows that majority of the respondents (45.3%) indicated that cyber attacks is the major consequence of non-compliance to cyber security among civil servants in Awka South, (37.2%) posited that security breaches is the major consequence of non-compliance to cyber security among civil servants in Awka South, (35.1%) opined that data loss is the major consequence of non-compliance to cyber security among civil servants in Awka South, (24.8%) indicated that low productivity is the major consequence of non-compliance to cyber security among civil servants in Awka South, (22.1%) indicated that bad public image is the major consequence of non-compliance to cyber security among civil servants in Awka South. This finding is corroborated by the data gotten from the IDI.

An interviewee posits that
Non-compliance to cyber security among civil servants in Awka South has a lot of consequences some of which are data loss and data theft. Others include loss of job and hardship and loss of revenue to the organization thereby affecting the public image and revenue target of the organization (Male, 27, Married, Awka, Urban).

Another interviewee stated:
To me there is a positive relationship between non-compliance to cyber security and data loss in the civil service. I believe that non-compliance to cyber security safety tips often leads to avoidable consequences such as identity theft, cyber attacks, data loss and low productivity. Also, non-compliance to cyber security affect employees' attitude to work and may lead to work rivalry and poor service delivery (Male, 37, Married, Unemployed, Awka Urban).

Discussions

The study seeks to examine internal and internal factors influencing cyber security compliance among civil servants in Awka South LGA. The study found out that there are internal factors influencing cyber security compliance among civil servants, some of which are; management policy on cyber security, computer literacy level, work ethics, improved supervision of workers e.t.c. This finding aligns with the study conducted by Madu (2020) whose findings state that the various internal factors influencing cyber security compliance among civil servants include: computer literacy, existence of office safety protocols, training and capacity building, safety manuals, punishment for non-compliance to cyber security practices, reward for compliance amongst others.
The study also found out that there are consequences of non-compliance to cyber security among civil Servants in Awka South. Some of the consequences include; data loss, bad public image, low productivity, security breaches and cyber attacks. This finding is in line with the study carried out by Yusuf and Ahmed (2020). Results

from the data showed that majority (70.0%) of the respondents indicated that one of the major consequences associated with non-compliance to cyber security among civil servants is data loss and data theft. Others include loss of job and hardship (20.0%) and loss of revenue to the organization thereby affecting the public image and revenue target of the organization. The study observed that when a breadwinner is fired for negligence of duty (non-compliance to cyber security), his family and other dependants will suffer hunger, poor health, complications and death in extreme situations. Also, the theoretical framework of the study explains this finding.

References

Ahmed, N., Kulsum, U., & Bin, A. (2017). *Cyber security awareness survey: An analysis from Bangladesh Perspective.* Dhaka, Bangladesh: Pan-Africa Press.

Alkalbani, A., Olusola, O. O., Alaba, F. A., Ogunleye, O. O., & Adebiyi, M. A. (2020). Factor influencing cyber security measures across the globe. *Journal of Cyber Security Systems, 2* (1), 3--10.

Amuta, C. (2020). Consequences of non-compliance to cyber security among civil servants in Warri, Delta State. *African Journal of Cyber Security, 2* (1), 5--7.

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cyber security management. *Journal of Cyber Security and Privacy, 1* (2), 219--238.

Awka History & Facts (2021). *Awka, history and facts.* Encyclopedia Britannica. Retrieved 2023-06-10.

Bergstrom, E., Lundgren, M., & Ericson, A. (2019). Revisiting information security risk management challenges: A practice perspective. Journal of Information and Computer Security, 2 (1), 3--7.

Carder, J. (2018). Cybersecurity: perceptions and practices: A benchmark survey of security professionals in the U.S., U.K., and Asia-Pacific Regions. Retrieved on 7/3/2023 from *https://www.jassolution.com/document/LogRhythm/LogRhthm-cybersecurity[-practices-and-attitudes-benchmark.]{.underline}*

Chai, W. (2021). Confidentiality, integrity and availability (CIA triad). Retrieved 14 September, 2021, from *[https://whatis.techtarget.com/definition/confidentiality-integrity-and-availability-CIA10/3/2023.]{.underline}*

Chandarman, R., & Van-Niekerk, B. (2017). Students' cyber security awareness at a private tertiary educational institution. *The African Journal of Information and Communication, 1* (2), 133--155.

Chikwendu, S. C., & Oli, N. P. (2023). Human factors influencing compliance to cyber security practices by employees of public universities in Southeast, Nigeria. *International Journal of Information Security, Privacy and Digital Forensics,* Vol.7, No.1.

Chukwurah, I., Daniel C. J., Uzor, O. A., Iwuno, J. O., Chukwueloka, I., & Chioma, I. (2020). Capacity building and employee productivity in the Nigeria public sector: A study of Anambra State Civil Service Commission, Awka. *International Journal of Advances in Engineering and Management, 2* (1), 299--308.

Effiong, E. (2021). Nigeria becomes world's second highest producer of cybercrime behind US. Techpoint Africa. Retrieved 20/09/2023 from: *[https://technpoint.africa/nigeria-second-highest-cybercrime-producer/]{.underline}*

Fasilat, A. S., & Satirenjit, K. J. (2021). Assessment of top management commitment and support on IS risk management implementation in the business organization. *Journal of Cyber Security, 2* (1), 3--10.

Ferreira, K., & Serpa, D. (2019). *Factors promoting the use of cyber security policies among workers.* London: Homeland Books.

Gana, N. N., Abdulhamid, S. I. M., & Ojeniyi, J. A. (2019). Security risk analysis and management in banking sector: A case study of a selected commercial banks in Nigeria. *Journal of Banking and Finance, 28* (1), 11--15.

Ghosemajumder, S. (2017). You cannot secure 100% of your data 100% of the time. Retrieved 7/3/2023, from *[https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time.]{.underline}*

Gilheany, T. (2017). It is time to change your perception of the cyber security. Retrieved 7/09/2023 *[from https;//www.securitymagazine.com/articles/87833-its-time-to-change-your-perception-of-the-cybersecurity-professional.]{.underline}*

Girma, A., & Lemma, L. (2020). *Human factors influence in information systems security: Towards a conceptual framework.* Harare: County Press.

Huyghue, B. D. (2021). *Cyber security, internet of things and risk management for businesses.* Utica College: College Press.

Kostyuk, N. & Wayne, C. (2019). C*ommunicating cyber security: Citizen risk perception of cyber threats.* Michigan: Michigan University.

Madu, C. (2020). Nigeria leads in Africa's cybercrimes. The Guardian. Available 21/10/23 at *[http://guardian.ng/business-services/nigeria-leads-in-africas-cybercrimes.]{.underline}*

Maisikeli, S. (2020). UAE cyber security perception and risk assessments compared to other developed nations. *2020 3^rd^ International Conference on Information and Computer Technologies (ICICT).*

Nnonyelu, A. U. (2009). Challenges of sustainable development. *Journal of Industrial Sociology, 2* (1), 10--15.

Odey, J. A. & Onebieni, A. P. O. (2021). *A survey on the perceptions and awareness of cyber security in Nigeria. Journal of Science, Engineering and Technology, 8* (1), 20--21.

Robbins, P. (2001). Models of health behaviour and clinical interventions in aging: A contemporary approach. *Journal of Clinical Interventions in Aging*, *1* (5), 19--22.

Ugbe, U. M. (2021). *Exploring the security measures to reduce cyber attacks within the Nigerian banking sector.* Enugu: Fourth Dimension Publishers.

Yamane, T. (1967). *Elementary sampling theory*. New York, NY: Practice-Hall.

Yusuf, S., & Ahmed, A. B. (2020). *Problems associated with non-compliance to cyber security among civil servants in six area councils of the F.C.T. (Federal Capital Territory).* Abuja: Fountain Press.