Cybersecurity Protocols and Threat Mitigation Strategies of Select Media Organisations in Abuja, Nigeria

Sharifatu Gago Ja'afaru & Kelvin Inobemhe
Department of Mass Communication
Glorious Vision University, Ogwa, Edo State, Nigeria
(Formerly Samuel Adegboyega University)
Ogwa, Edo State, Nigeria
sharifatujaafaru@gmail.com

DOI: https://doi.org/10.5281/zenodo.14034385

Abstract
The researchers examined cybersecurity protocols and threat mitigation strategies of select media organisations in Abuja. In-depth interview was used as the research method to gather relevant qualitative data for the study. Anchored on the protection motivation theory, the researchers analysed how media organisations respond to cybersecurity threats. The findings showed that the media owe the society an obligation to gather and disseminate information so that citizens can have sufficient information to plan their lives and avoid danger. Findings further showed that the media in Nigeria are faced with cyber security threats; some of the threats identified are ransomware, credential theft and phishing attacks. It was further discovered that cybersecurity strategies put in place by the select media organisations are to a reasonable extent adjudged to be highly effective. It was concluded that there are identifiable threats to the cybersecurity of media organisations in Nigeria. Thus, there is need for media organisations to educate their staff on latest trends in cyber security in order to protect the confidentiality, integrity and the availability of the information they disseminate on the superhighway.

Keywords: Cybercrime, Cybersecurity, Cyberspace, Media, Mitigation Strategy

Introduction

The age of digital-driven information has simplified global communication and activities; it creates large-scale opportunities for nations to thrive, thereby promoting national growth. The increasing sophistication of the digital environment constitutes a notable challenge for organisations worldwide, making cybersecurity a critical concern. Protecting communication systems is no longer just a requirement; it has become a necessary step to achieving secured communication in today's changing landscape. Modern digital technologies facilitate faster and more versatile communication than ever before. Whether one is disseminating business information or circulating office briefings, communication devices are used in different sectors, including educational institutions, health institutions, financial institutions, transportation sector, businesses, agriculture and governments globally. With the growing impact of these outcomes, the imperative to guarantee their security becomes more pronounced.

The cyber-age facilitates corporate transactions, but it is also vulnerable to an increasing number of cyber-attacks, which could undermine the effectiveness of the system and its developmental contribution to the process of national growth. When

vulnerabilities in users' operating systems, networks, and processes are taken advantage of, attacks could occur. As technology becomes more effective and user-friendly, the proficiency of cybercriminals equally intensifies. A critical concern lies in the fact that innovative technologies, designed to perform versatile functions are frequently dependent on additional tools or services, which fundamentally introduce numerous potential attack vectors. These flaws could be used to steal, disrupt or obtain unauthorised access to information, features or services. Regrettably, it is undeniable that with the advent of new technologies, there come masked vulnerabilities (Dillon, Lothian, Grewal & Pereira, 2021; Ikuero & Zeng, 2022; Partida, 2021).

According to CrowdStrike Global Threat Report (2021), cybersecurity incidents grew by 400% from 2019-2020 and most incidents involved cybercriminals. Governments, businesses, financial institutions, military organisations, and healthcare organisations frequently collect, assess, analyse and store enormous volumes of data on computers and other devices, making cybersecurity essential. A large portion of this data may contain sensitive information, such as financial, personal, intellectual property, or other types of data that, if accessed or exposed illegally, could have dire repercussions (Longe, 2022). Put in another way, a breach of the database could potentially pose varied degrees of danger to data that may range from personal to organisational and even intellectual.

Unquestionably, a substantial digital revolution was under way even prior to the COVID-19 pandemic. Attacks based on phishing (cybercriminals disguising and sending false emails to their victims) and ransomware (paying an amount of money to cybercriminals in exchange for one's stolen data) were a major threat. Businesses were moving toward the cloud and were tenacious in their attempts to take over the cybertalent market. Executives were able to hear from cyber leaders. Attackers have been focusing more and more on industries like healthcare, education, and manufacturing in addition to the financial sector (Dillon *et al* 2021). The negative impact and dimensions were of significant impact at both the individual and corporate levels. This is another angle of concern for data security in modern times.

According to Dillion *et al* (2021), the condition prevailing prior to the onset of the COVID-19 pandemic was already risky. In its 2019 annual report, Accenture highlighted the escalating sophistication and professionalism of threat actors, who were increasingly focused on exploiting global events as opportunities to target people in various ways (Accenture Security, 2019, as cited in Dillion *et al* 2021). Between 2015 and 2018, the number of people using the internet doubled from 2 billion to 4 billion and this is considered as an extraordinary increase (Morgan, 2019 Official Annual Cybercrime Report, as cited in Dillion *et al* 2021). Additionally, "the number of Internet of Things (IoT) devices connected to the worldwide web was steadily rising and anticipated to reach 50 billion by the end of 2020" (Evans, 2011, p. 3). This makes the vulnerability of systems more predictable.

In the media, especially in the digital age, where even the traditional media organisations have online presence, the need for a well-policed digital space continues to rise. This is because cyber threats to media organisations are said to be on the rise

globally (Peck, 2022). More than ever before, journalists and global news media are faced with a greater cybersecurity and digital security threats as they are targets for spyware, malware and digital surveillance putting the personal information of their sources at risk of being compromised (Center for News Technology & Innovation, 2024). This issue is not restricted to the global media alone as news media in Africa in general and Nigeria in particular are also faced with threats of similar fashion (Kabir, 2022). Such attacks may be sponsored by the authorities or from other elements with vested interest. On the backdrop of the foregoing, this study tests their preparedness. Therefore, this study is focused on media organisations in Nigeria to learn their threat mitigation strategies and cybersecurity protocols.

Statement of the Problem

Cyberspace presents endless possibilities for diverse human activities, encompassing social, economic, educational and political, health and agricultural spheres within society. Internet technology created an era where human activities, financial transactions, technical operations, and communication processes continuously move into the digital realm, the persistent threat of online susceptibility and cyber-attacks continues to cast a shadow over the virtual landscape. While cybersecurity has always been a central facet of computing systems, its importance has surged in recent times (Longe, 2022). The world is faced with different reports of cyber-attacks that take on different dimension and a wide range of institutions; the financial sector, health and many more including the media.

In sub-Saharan African, Nigeria, Ghana, and South Africa are identified as leading in cybercrime (Ajao, 2008, as cited in Olayemi, 2014). It is rare to find a location with computers and internet access where there are no recorded criminal cases. Idowu & Madaki (2021) expressed frustration that young people in Nigeria are now heavily involved in cybercrime. The problem is threatening the nation's socioeconomic progress and has deeply ingrained itself into our society. It is important to note that while cybercrime is an international problem, the vulnerabilities and effects vary according to how strong the defenses each nation puts in place against the threat, such as cyber laws and cyber protection technology (cybersecurity).

Regrettably, as the aforementioned arguments demonstrate, Nigeria is highly affected by cybercrime, and the country's efforts to lessen cyberthreats are still limited because of insufficient cybersecurity expertise, outdated technology, and lax cybercrime laws. The media cannot to be compromised on account of poor cyber security. Aside the danger of compromising information source that may be in raw file format, there is also the threat of modifying posted information and news on the websites of news organisations. According to Kabir (2022), news media websites in Nigeria continue to face cyber-attacks for holding authorities accountable. The attack could be multidimensional and may take on different dimensions. The outcomes presented from prior studies above are alarming and it is in order to limit and proffer solution to the challenges that the study looks at the cybersecurity protocols and threat mitigation strategies that are put in place to protect media organisations in Abuja, Nigeria.

Objectives of the Study

The objectives of the study were to:

1. Find out the cybersecurity threats troubling the select media organisations in Abuja Nigeria.
2. Ascertain the vulnerabilities of the media organisations to cybersecurity threats.
3. Evaluate incident response preparedness of the organisations towards the threats.
4. Identify the cybersecurity protocols and strategies employed by the select media organisations.
5. Determine the effectiveness of cybersecurity protocol in mitigating threats.

Conceptual Review

The process of defending against hostile attacks on servers, computers, mobile devices, electronic systems, programmes, networks and data from online threats is known as cyber security. It is also known as electronic data security or information technology security (Longe, 2022). Similarly, Moturi, Abdulrahim & Orwa (2021) aver that cybersecurity is the defense against assaults on the confidentiality, integrity and availability (CIA) of data and information systems. Cybersecurity ensures that the information infrastructure and assets of users or corporations are always safeguarded against any related hazards.

Cybercrime is a global phenomenon. It cut across geographical boundaries. These crimes are committed even when the main subject in the act is physically not at the crime scene. These crimes occur in the domain of information superhighway. To commit such crimes, all that is needed is a computer linked to the internet. Idowu & Madaki (2021) see cybercrime as acts that include hacking, publishing of information on electronic format without authorisation, violating confidentiality, publishing false digital signatures, interfering with systems, stealing, destroying or damaging computer source code, as well as illegal interception, access and misuse of devices for fraudulent activities. Therefore, breaches of personal and corporate data, harm to network integrity, invasions of privacy, industrial espionage, software piracy and other crimes where a computer plays a significant role in the commission of the crime are all considered forms of cybercrime.

The term "cyberspace" describes the online community and, more precisely, an electronic platform that promotes contact between users. Cyberspace's fundamental characteristic is that, it is an interactive and virtual sphere for a wide variety of users (Longe 2022). Another meaning of the concept of cybercrime is that of digital realm of computer networks, the Internet, and related forms of electronic communication and may also extend to a virtual space created for organisations and individuals to interact and share information on a global scale without the physical location being a barrier (Castillo, 2023). Additionally, it can also refer to a domain inside the information environment that is made up of separate networks of infrastructures for information systems, such as computer systems, embedded processors, controllers, and networks for communications (National Institute of Standards and Technology, 2012).

Media on the other hand are channels of information dissemination. According to Asemah (2011a, p. 36), "media are the channels through which messages travel from the source to the receiver." Before being sent to audiences, media messages are frequently

chosen and edited; viewers are not given any control over the media information to which they are exposed (Asemah, 2011b). Similarly, Asemah (2011b) observes that because of their propensity to "bark" when a problem arises, the media are frequently referred to as the society's watchdog. The media can be seen as a kind of flashlight, illuminating shadowy areas that some people would rather stay out of. To effectively and efficiently carryout this watchdog function, media organisations need to protect their communication systems, information and data against cyber threats and criminals.

Literature Review

The goal of cybersecurity is to protect cyberspace from attacks. The term "cyber-threat" is relatively vague and refers to a variety of malevolent actors using information and communication technology (ICT) either as a tool or as a target (Olayemi, 2014). Since cybersecurity will determine how we are seen in the global village, it is a fact that needs to be addressed immediately. The world of today is undergoing a tremendous transition that will result in all physical activities related to daily life being completed online, including financial transactions and the dissemination of news and information. Hence, it is paramount to recognise the ardent cybersecurity issues presently affecting technology (Ajie, 2019; Ekanayake, Karunarathna, & Miyuranga 2020; Olayemi, 2014). And by technology we mean across different spheres of human activities, including banking, media, commerce, and many more.

Idowu & Madaki (2021) aver that the definition of cybercrime is varied. Hence, it is contextual in nature. Erhabor (2008) notes that cybercrime refers to one of the hastiest rising criminal activities presently seen in the world. According to Dennis (2024), cybercrime involves the use of the computer as the tool to further illegal ends, which may include (but not limited to) identity theft, intellectual property theft, trafficking in child pornography, invasion of privacy, and fraud. Furthermore, it also encompasses a wide range of illicit activities, such as tracking, downloading pornographic photos from the Internet, financial frauds, virus attacks, computer hacking, and building websites that incite hatred. Additionally, Nigeria is not immune to the damaging effects of cybercrimes.

With the increasing number and complexity of cyber-attacks, businesses and organisations, especially those tasked with protecting national security, health, information or financial data have discovered the need to strengthen their efforts in intensifying the fortification of sensitive business and personal information (Longe, 2022). Strictly speaking, since 2001, cybercriminals have stolen or caused losses totaling a staggering $3.5 trillion (Clement, 2020) thanks to a constant ransomware outbreak that has affected all organisations and areas and stolen identities. Even in a world that was generally safe and peaceful, it would have been reasonable to anticipate that cyber-attacks would become more difficult given the circumstances at the beginning of 2020. And this calls for an end to the menace as experts and concerned individuals have called for its total eradication through a treaty that criminalises crimes dependent on cybercrimes (Wilkinson, 2023) or at least an increase in efforts to do so.

Hence, Idowu & Madaki (2021) note that in order to eradicate cybercrime in Nigeria, several attempts have been made by government which includes: enactment of cybercrime (preventing prohibition etc.) Act, 2015; Economic and Financial Crimes Commission (Est.) (EFCC) Act 2004; constitution of the Federal Republic of Nigeria 1999 (as amended); Advance Free Fraud and other fraud related offences (AFF) Act 2006; Nigerian Communication Act 2003; Money Laundering (Prohibition) (Amendment) Act 2012; National Information Technology Development Agency (NITDA) Act 2007; Evidence Act 2011, and so on. These are laws established to bring the activities of cyber criminals to a halt or at least mitigate their impacts.

Regardless of all these laws and formations, the tide of cybercrime in Nigeria is still excessive. News outlets in Nigeria and other countries such as Philippines, Kosovo, Kyrgyzstan are reportedly targets of a type of attack known as DDoS an acronym for distributed denial-of-service attack with the use of RayoBytes's services (*Premium Times*, 2023). Aside the foregoing, media businesses have also suffered a number of attacks from cybercriminal in recent times (George, 2023; Leyden, 2024). In Nigeria, cybercrime has a very significant effect on per capita income. It supports any illicit activity carried out by one or more individuals utilising networked computers, phones, and other information and communications technology (ICT) devices to access the internet. These individuals are known as scammers, hackers, online fraudsters, cyber citizens, or 419ners. Cybercriminals attack entire networks as well as computers, tablets, and mobile phones (Adesina, 2017, as cited in Idowu & Madaki, 2021).

The Nigeria Computer Emergency Response Team (ngCERT) was formed by the Federal Government of Nigeria (FGN) to manage incident response and mitigation plans in order to stop cybersecurity incidents in Nigeria. Also, it developed the National Cybersecurity Policy and Strategy and drafted the Cybercrimes (Prohibition, Prevention Act, 2015) (NCPS 2021, as cited in Falode, Faseke & Ikeanyichukwu, 2021). The implementation of security policies and processes to lessen the impact of cybersecurity risks in organisations, countries, and the global community is known as cybersecurity threat mitigation (Calderaro & Craig 2020; Olayemi, 2014). These days, any organisation that is cyber-literate and conducts business online must prioritise reducing cybersecurity threats (Saulawa & Abubakar, 2014; Thompson, 2018).

Theoretical Framework

The protection motivation theory (PMT) serves as the theoretical foundation for this study. A popular paradigm for comprehending reactions to stimuli that make people perceive a possible threat is protection motivation theory. Among these triggers are fear messages that advise people to take precautions or abstain from actions that could endanger themselves or others (Shillair, 2020). The psychological threat theory (PMT), developed by R.W. Rogers in 1975, holds that people's desire to defend themselves against threats is based on how they view their cognitive assessment of the threat and their capacity to deal with it. Applying the theory to comprehend and forecast health-related behaviours and guide the creation of successful health promotion interventions

has become commonplace (Conner & Norman, 2015, as cited in Marikyan & Papagiannidis, 2023).

In the context of this study, the theory was used to analyse how media organisations respond to cybersecurity threats. This idea, according to Shillair (2020), is a part of the expectancy-value theories, which hold that attitudes or beliefs will influence actions in the future. PMT theorises that people assess possible answer using a threat analysis and coping evaluation process. The process of evaluating a danger involves determining its level of severity as well as its probability or vulnerability. The effectiveness of the reaction, its difficulty to implement (such as its cost) and the perceived self-efficacy of doing so are all taken into account during the coping assessment process. A maladaptive response occurs when the threat appraisal outweighs the coping evaluation. This can involve denying it, downplaying the danger or choosing to ignore it. Protection motivation is attained if the coping response, which consists of perceived self-efficacy and belief in response efficacy, is stronger.

The theory is relevant to this study in the sense that it provides significant understanding to how media organisations identify and aptly respond to cyber threats. It facilitates the examination of thought processes that push organisations to evaluate the seriousness of a threat, their weaknesses and to decide the most potent and viable defense strategies. In addition, PMT draws attention to the driving forces influencing the acceptance and continuing implementation of cybersecurity formalities in our contemporary societies shedding light on the need as well.

Methodology

The researchers adopted the interview research method. The research design is suitable for this study because according to Asemah, Gujbawu, Ekhareafo & Okpanachi (2012, p. 123), "when conducted properly, the interview as a tool of data collection can yield deeper and more reliable information than the questionnaire." Hence, the whole essence of conducting an interview is to obtain relevant data that can help in achieving the set objectives of the study. The area of study for this research is Abuja metropolis which encompassed Asokoro, Central Area, Garki, Maitama and Wuse districts respectively (Adama, 2020). This is because the metropolitan area hosts the headquarters of different media organisations. Accordingly, four professionals (IT experts) from different media organisations with in-depth understanding of cybersecurity were purposively selected for the in-depth interview (IDI). For this study, four (4) media organisations were selected which include two apiece of print and broadcast genre namely, Daily Trust Newspaper, Guardian Newspapers, Nigerian Television Authority (NTA) and African Independent Television (AIT).

The explanation building model was adopted to analyse the data gathered from the twenty-five minutes IDI conducted with each of the interviewee. Propounded by Yin (1984), the explanation-building model shows that the approach is handy when qualitative data are to be presented chronologically. For a study of this nature that entails a detailed explanation in to how cybercriminals operate and how they carry out their heinous acts, the explanation building model becomes suitable.

Data Presentation/Analysis

The study yielded adequate data from the IDI conducted with the IT experts in the select media organisations in Nigeria. The nature of the data informed the use of thematic presentation of findings with the use of explanation building model. Five theme areas were determined in line with the objectives of the study.

Cybersecurity Threats Troubling Select Media Organisations

Media organisations in Nigeria are faced with cybersecurity threats, ranging from phishing attacks to credential theft. This is common because of the changing information system in our globalised world. A participant laid bare the kinds of cybersecurity challenges troubling their organisations and stated that:

> The cybersecurity threat we face will be because of our operational environment, being a media house. We are a media house and also an organisation, we have different systems that you basically find in our organisation; from enterprise resource management to the different platforms we use for our media operations and down to the different platforms we use to disseminate the information we generate internally, so for each one of them and also entirely, they also have their own set of threats individually facing them and also a general set of threat. Basically a threat you find with every system on the Internet is applicable, things like Distributed Denial of Service (DDoS) attack and the rest of them, credentials, hijacking and down to ransomware, Phishing attack, so you have different environment and for internal application, we are looking at control access, hijacking, credentials stealing, social reengineering and things like that so, depending on what platform or what angle, we have different forms of threat facing each of those different systems. (Mr. Auwal Abdullahi, Male, Media Trust Group, 2024)

The issues go deeper to personal problems from individual users and their system. The 21st century internet environment is one replete of identity theft and false identities of so many users. In line with the foregoing, a respondent noted that "basically, the basic threats we face in cybersecurity aspect are malware, information disclosure and issues of fake account. But the most prevalent is the issue of fake account" (Taminu Adamu, Male, NTA, 2024). It is evidently clear that the issues are also on a personal level as much as they are institutional.

Additionally, respondents revealed more in respect of the kind of cybersecurity threats faced by the media organisations. In line with the foregoing, the respondents noted with the assertion that:

> As a media organisation just like every other public organisation, we are exposed to such threats because the hackers are on the lookout every moment for organisations that can fall in their trap and my organisation is among those categories of organisations they look out for and we see a lot of these threats on a daily basis. Cyber-attack threats like Distributed

> Denial of Service (DDoS) attack, ransomware, malware attack (Chinedu Ogbonna, Male, *Guardian Newspaper*, 2024)

> We do not really have much in the electronic media unlike the print media and social media but, the few three encounters are: ransomware, phishing - these happen generally across the globe where by people tend to impersonate through emails; mobile security attack. That is our mobile App (AIT Mobile App), people develop a similar app, which is actually different from ours but the same identity. If you have to go to Google playstore to download this app, you may be looking for AIT, if you are not familiar with the one that is for AIT, you can mistakenly download a fake app and once you install it into your system; you are already vulnerable to attack. We also have the issue of identity theft, which is people tending to impersonate a brand, people claiming to be AIT staff when they are not (Abodunrin O. B. James, Daar Communications, 2024).

These threats are not just ordinary; they go deeper than just the surface implications as they impact negatively on the entire information architecture of media organisations in Nigeria. The rippling effect could also extend to lack of trust from sources that may develop fear that their cover and anonymity may not be guaranteed after all.

Vulnerabilities of Media Organisations to the Cyber Threats

Another area of focus of this study is the vulnerabilities of the select media organisations. In addition, the focus also tilts to ascertain how dangerous the negative consequences of the threats will be on the end-users of the cyber space. Interviewee avers that:

> From the systems we use and how we also operate the systems, we have a decent existing system security wise, thus if you ask me how vulnerable are our online systems, I am basically very confident apart from two aspects which you really cannot do much about, depending, that is because first, however you position your system, you must likely have limited resources. Secondly, you have human beings actually using these systems that can also be a bone of contention. (Mr. Auwal Abdullahi, Male, Media Trust Group, 2024)

In the digital world and with the internet and networks provided in 21st century, there may be no guarantee of total security across the web. On this note, another interviewee remarked that:

> Nobody has 100% immunity when it comes to cyber threats. Reason being that the hackers and all the people trying to attack are always trying to devise different means and new methods of attacking – and likewise those who are doing the preventive and protective measures always try to bring new application or ways. In our own case, we can say we are near to no vulnerability. (Taminu Adamu, Male, NTA, 2024)

Furthermore, the ever-challenging internet space and its dynamic users put the world at constant risk. The actions of Cyberattackers are predictable and this also calls for equal reaction from those that own and maintain the different domains that may be at risk of being attacked. Consequent upon the foregoing, one of the interviewees remarked thus:

> We are always a step ahead and putting measures in place because even as we speak, these threats keep coming out in different forms as the day goes by. When you have a policy today, by tomorrow you need to upgrade to meet up with the future challenges. It is an ongoing concern (Chinedu Ogbonna, M, *Guardian* Newspaper, 2024)

Vulnerability of the media organisations to cyber threats are of varied level and degrees. This was the case of the position of an interviewee who asserted that "the threats are not so high; they are at a very low rate" (Abodunrin O. B. James, Daar Communications, 2024).

Incident Response Preparedness of the Organisations towards the Threats

As seen from the data captured above, the cyber threats to media organisations in Nigeria are real. What is uncertain is how prepared the users or hosts are toward mitigating and neutralising these threats in the face of a growing sophistications in the knowledge and technology used to carry out such attacks. Interviewees noted that:

> This I can tell you from experience, the most effective one has been the proper disaster recovery plan that is the most effective and reliable incident response. Essentially you try to make sure you have proper isolated and tested back-up that you can easily recover from should you have a total system failure that is the first thing. The second thing is always have a primary and auxiliary line of communication to your users. Basically somewhere where you can keep them abreast of what is happening. Ok, system is down, should they use the system, what kind of data should they key in, should they not key in data, is something going wrong, and the responses? I think it is good to have that line of communication, because should there be an incident, it can really hamper operation, but the whole idea is to try to minimise the effect if such happened, so keeping a clear line of communication after disaster recovery (Mr. Auwal Abdullahi, Male, Media Trust Group, 2024)

According to the results of one of the IDI sessions, there are other recommendations that come handy and helpful in efforts to mitigate the cyber threats troubling media organisations in Nigeria. Accordingly, a respondent stated thus: “we use the four phases of National Institute of Standards and Technology (NIST) it is a framework that has been put in place to mitigate the cybersecurity threats” (Taminu Adamu, Male, NTA, 2024).

The issues are as numerous as the steps to mitigate them. Put in another way, the threats are numerous and so are the solutions. It is important to note that nothing can be done without proper planning and preparation by the owners of the different platforms at risk of attacks.

Cybersecurity Protocols and Strategies Adopted by the Media Organisations

The protocols and strategies deployed to fight the cyber threats faced by the media organisations make up another significant area of this study. The enquiries also yielded important results. In line with the foregoing, an interviewee stated that:

> When it comes to development and acquisition, we try to as much as possible review the entire process for the acquisition of development itself and to safeguard against things like threats coming from supply chain attack, compromised vendors or internal threat and also possibly physical threat. We just try to have extensive review of the entire process before any acquisition or development, then also our IT support team do a sort of internal digital sensitisation for our staff basically trying to raise awareness and also give them tips on how to handle themselves digital security wise; that is, online security wise (Mr. Auwal Abdullahi, Male, Media Trust Group, 2024)

The overall goal is to block all efforts to hack and destabilise the systems of the media organisations. A respondent talked about the simplest of protocols deployed as part of efforts to mitigate threat. The respondent mentioned "Firewall, two step verification and the https" (Taminu Adamu, Male, NTA, 2024) as the protocols and strategies deployed to ensure a safe database and system for the media organisations. The importance of a firewall in internet and data protection efforts cannot be overemphasised and so IT departments of the different organisations also share similar knowledge.

The acquisition and maintenance of alternative broadcast means or channels is one other significant strategy that can be adopted to mitigate cybersecurity threats posed by different groups the world over. In addition, there is also the strategy that emphasises regular monitoring of login credentials to ensure that there is no breach. One of the best ways to be secured from that angle is to always check the login sequence and update where necessary.

Effectiveness of Cybersecurity Protocols in Mitigating Threats

For a system/strategy/protocol to be successful, it must achieve its primary goal as set out by the media organisation. Therefore, the enquiry on the cybersecurity protocols and strategies and their effectiveness also yielded quite a number of important results. One of the interviewees noted thus:

> Looking at what has been happening because we have dealt with ransomware and some data loss and all, I will say we are much more effective at mitigating or recovering from such incidents, and now, they rarely happen more or less; let me not say it is impossible to happen again,

> I will say it has been pretty effective so far. There is still room for improvement, but it has been effective (Mr. Auwal Abdullahi, Male, Media Trust Group, 2024)
>
> It is very effective because since we started online operations in 2013/14 (from our websites to all our social media platforms), we have never had any successful attack (Taminu Adamu, Male, NTA, 2024)

Many of the interviewees noted that strategies and protocols designed to mitigate attacks can only be effective if they have the capacity to stop successful attacks and intrusion by an external aggressor. ‘‘Well, since we started implementing these measures, we have not had any serious effect, as an organisation. We have not had any attack that has crippled our operations, but we are always moving ahead of time to ensure that all the things we need to put in place are done on time to prevent future occurrence because it is a growing concern’’ (Chinedu Ogbonna, M, Guardian Newspaper, 2024).

Discussion of Findings

The findings showed that on account of the operational environment of the media organisations and global trends in the cybercrime world, they are faced with threats such as distributed denial of service (DDoS), ransomware, phishing attacks, credential theft, malware attacks, false identity, mobile security attacks and so many others. The implication of the foregoing is that the cybersecurity threats to the internet users, including media organisations are real. It is instructive to state that these threats pose serious challenge to media practice anywhere in the country. This is a validation of an earlier assertion by the Centre for News Technology and Innovation (2024) that publishers and journalists across the world are considered as high-profile targets for all types of cyber security threats.

Furthermore, the findings also showed that though the select media organisations (*Daily Trust*, NTA, Guardian Newspapers and the AIT) appear somewhat prepared for any type of cyber threat, the global warfare against organised systems by cybercriminals is evolving and the threats glaring. This also implies that there are some threats that are always there and the IT personnel must always watch out for such and prepare for any eventuality. Some of the media organisations have layers of firewalls preparatory for any form of eventuality. This makes them way prepared for cyberattacks devising means to mitigate the impact and reduce the adverse effect on the IT assets as well as the information breach to the barest minimum. This aligns with the position of scholars that advocated the use of layers of firewalls for protection from cyber threats (Fulp, 2014; Schwartz, 2023; Yasar, 2023). Indeed, the standard is to ensure data protection in the media and firewalls provide a part of that.

Additionally, the findings also showed that there are active and existing strategies and protocols aimed at mitigating cyberattacks in the select media organisations in Nigeria. Although, media organisations are susceptible to compromise due to cybersecurity threats, the study discovered that, the media organisations have a proper and potent existing security system. These strategies put some organisations at a “near to no vulnerability” while some have very low rate of threats as the study discovered.

Personal digital security is encouraged; that is, how users handle their credentials is a crucial area in making one vulnerable because cyber threats are continuously evolving. The findings showed that no media organisation is immune to that. Some acknowledged being vulnerable to Trojan horse virus, malware and ransomware attacks. The foregoing is in line with existing knowledge on the fact that there is no immunity anywhere for organisations in respect of cyber threats (Simpson, 2020; Warrillow, 2024)

However, no matter the measures put in place, there are limiting factors that make an organisation susceptible to cyber threats. The physical hardware or virtual hardware systems inevitably makes an organisation vulnerable and human beings using these systems are also points of vulnerability. This implies that the vulnerability of the select media organisations under study is at a very low rate because of the functional security frameworks and policy put in place to protect data, information, systems and networks. The researchers identified proper disaster recovery plan as the most effective and reliable incident response. This refers to proper isolated and tested back-up that an organisation can easily recover from in the case of total system failure, having systems to switch back to, both from online platforms and network infrastructure to keep partners informed of situations when faced with threats.

Another incident response plan the study unraveled is organisations using the four phases of National Institute of Standards and Technology (NIST) framework. Blacklisting email address from back end server, checking of identity and changing of passwords, subscribing to more than one satellite provider, are among the incident level preparedness put in place by organisations to reduce the effect of the threat because it cannot be totally eliminated. The implication of the above is that, no matter how prepared an organisation may be against cyber threats; it will keep evolving and need to be abreast to curtail it and protect their presence on the superhighway. This agrees with positions that threats will always persists in the cyberspace no matter how prepared an institution/organisation may be (Liu *et al* 2022; Ursillo & Anold, 2023).

Media organisations in Abuja are at the forefront of protecting their business, interest and reputation. Thus, they employ some protocols and strategies to lessen the effects of cybersecurity threats. The findings showed that firewall, two-step verification and the https are some of the protocols employed by media organisations in Abuja to mitigate threats. Agreeing with the foregoing, some scholars also advised the use of https and firewalls and many more as defense strategies against cyberattacks (Deshpande, 2023; Gordon, 2023).

Findings further showed that the cybersecurity protocols of the select media organisations in Abuja have been effective.

Conclusion and Recommendations

The researchers conclude that the select media organisations have effective cybersecurity protocols and strategies put in place to safeguard their organisations against cyber threats. Based on the findings and conclusion, the researchers recommend that there is need for special training programmes to teach media practitioners the dangers posed by cybercriminals in our world and ways to mitigate such threats. Media organisations

should endeavour to educate their staff, especially those in IT sections on a regular basis on new trends and threats and new ways to tackle them. This can be through avenues created for training and re-training of staff in collaboration with internationally-certified organisations that specialise in data protection.

References

Adama, O. (2020). Criminalising informal workers: The case of street vendors in Abuja, Nigeria. *Journal of Asian and African Studies*, 56(3), 533-548. Retrieved from https://doi.org/10.1177/002190962093074.

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science*, 13(4), 19-29.

Ajie, I. (2019). A review of trends and issues of cybersecurity in academic libraries. *Library Philosophy and Practice (e-journal)*. 2523. Retrieved from https://digitalcommons.unl.edu/libphilprac/252

Asemah, E. S. (2011a). *Selected mass media themes*. Jos: University Press.

Asemah, E. S. (2011b). *Mass media in contemporary society*. Jos: University Press.

Asemah, E. S., Gujbawu, M., Ekhareafo, D. O. & Okpanachi, R. A. (2012). *Research methods and procedures in mass communication*. Jos: Great Future Press.

Calderaro, A. & Craig, A, J. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), 917-938.

Castillo, J. A. H. (2023). Cyberspace origin, applications and examples. *Study.com*. Retrieved from https://study.com/academy/lesson/cyberspace-history-origin-overview.html

Centre for News Technology & Innovation. (2024). Journalists and cyber threats. Retrieved from https://innovating.news/article/journalists-cyber-threats/

Clement, J. (2020). Internet usage worldwide – statistics and facts. Retrieved from https://www.statista.com/

CrowdStrike. (2021). Global Threat Report. Retrieved from https://www.crowdstrike.com/press-releases/global-threat-report-highlights-ecrime-trends-and-nation-state-activity/

Deshpande, C. (2023). What is firewall: Types, how does it work, advantages & its importance. Retrieved from https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall

Dillon, R., Lothian, P., Grewal, S. & Pereira, D. (2021) Cyber Security: Evolving threats in an ever changing world. In A. Kuah, & R. Dillon (Eds*.). Digital Transformation in a Post-COVID World: Sustainable Innovation, Disruption and Change* (pp. 129-154). Florida: CRC Press

Ekanayake, N. K., Karunarathna, H. M. & Miyuranga, R. (2020). What is cybersecurity: The reality of modern threats. Retrieved from https://www.researchgate.net/publication/338385940

Erhabor, I. M. (2008). Cybercrime and the youth (PGDE Thesis), Department of Education, Ambrose Alli University, Ekpoma, Nigeria.

Evans, D. (2011). The Internet of things: How the next evolution of the Internet is changing everything. CISCO White Paper, 1, 1-11.

Falode, A. J., Faseke, B. O. & Ikeanyichukwu, C. (2021). Artificial intelligence: The missing critical component in Nigeria's security architecture. *SSRN*, 3896657

Fulp, E. W. (2014). Firewalls. In J. R. Vacca (Ed.), *Managing Information Security* (Second Edition). Elsevier. Retrieved from https://doi.org/10.1016/C2011-0-08782-3

George, G. (2023, Apr. 2). Bank customers, companies lose billions to Nigeria's weak cybersecurity. *The Punch*. Retrieved from https://punchng.com/bank-customers-companies-lose-billions-to-nigerias-weak-cybersecurity/

Gordon, K. (2023). Firewall – not your best cyber defense strategy (part 1). *LinkedIn*. Retrieved from https://www.linkedin.com/pulse/firewall-your-best-cyber-defense-strategy-part-1-kevin-gordon

Guanah, J. S. & Guanah, J. S. (2022). Mass media and cyber security in the maritime industry: Analysing the threats and prevention. *Global Journal of Arts Humanity and Social Sciences*, 2(2), 63-73.

Idowu, O. A. & Madaki, M. (2021). Cybercrimes and challenges of cyber-security in Nigeria. *Fuwukari International Journal of Sociology and Development*, 3(1), 1-12.

Ikuero, F. E. & Zeng, W. (2022). Improving Cybersecurity incidents reporting in Nigeria: Micro and small enterprises perspectives. *Nigerian Journal of Technology (NIJOTECH)*, 41 (3), 512-520. Retrieved from http://dx.doi.org/10.4314/njt.v41i3.10

ITU. (n.d.). Introduction to security cyberspace, cybercrime and cybersecurity. *AfricaCER*T.

Kabir, A. (2022). Nigerian news websites continue to face massive cyber attacks for holding authorities accountable. *HumAngle*. Retrieved from https://humanglemedia.com/nigerian-websites-continue-to-face-massive-cyber-attacks-for-holding-authorities-accountable/

Layden, J. (2024). Nigerian businesses face growing ransomware-as-a-service trade. *Dark Reading*. Retrieved from https://www.darkreading.com/cyberattacks-data-breaches/nigerian-businesses-face-growing-ransomware-as-a-service-trade/

Liu, X, Ahmad, S. F, Anser, M. K, Ke, J., Irshad, M., Ul-Haq, J. & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, 19(13):927398. Retrieved from https://doi.org/10.3389/fpsyg.2022.927398

Longe, O. B. (2022). *Cyber security*. Abuja: NOUN.

Marikyan, D. & Papagiannidis, S. (2023) Protection motivation theory: A review. In S. Papagiannidis (ed.). *Theory hub book*. Retrieved from https://open.ncl.ac.uk /

Moturi, C. A., Abdulrahim, N. A. & Orwa, D. O. (2021). Towards adequate cybersecurity risks management in SMEs. *International Journal of Business and Risk Management*, 11(4), 343-366. Retrieved from https://doi.org/10.1504/IJBCRM.2021.119943

National Institute of Standards and Technology. (2012). Information security. Guide for conducting risk assessments. Gaithersburg: Department of Commerce, United States of America. Retrieved from https://doi.org/10.6028/NIST.SP.800-30r1

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3), 116-125.

Partida, D. (2021). The importance of cyber security for mass communications systems. Retrieved from https://www.cybertalk.org/2021/03/17/the-importance-of-cyber-security-for-mass-communications-systems/

Peck, G. A. (2022). Cyber threats to media companies are on the rise. *Editor and Publisher*. Retrieved from https://www.editorandpublisher.com/stories/cyber-threats-to-media-companies-are-on-the-rise,225421.

Premium Times. (2023, Sept. 8). Cyberattackers used US company to crash media sites in Nigeria, others. Retrieved from https://www.premiumtimesng.com/news/top-news/623974-cyberattackers-used-us-company-to-crash-media-sites-in-nigeria-others.html?tztx=1

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change1. *Journal of Psychology*, 91 (1), 93-114.

Saulawa M. A. & Abubakar, M. K. (2014). Cyber-crime in Nigeria: An overview of cybercrime act 2013. *Journal of Law, Policy and Globalisation*, 32. 23-33.

Schwartz, D. (2023). The layers of cybersecurity: Is your company covered? Retrieved from https://www.forbes.com/sites/forbestechcouncil/2023/05/09/the-layers-of-cybersecurity-is-your-company-covered/?sh=740dcca95774

Shillair, R. (2020). Protection motivation theory. Retrieved from https://doi.org/10.1002/9781119011071.iemp0188

Simpson, C. (2020). Why no business or sector is immune from cyber threats. Retrieved from https://www.allianz.co.uk/news-and-insight/insight-and-expertise/why-no-business-or-sector-is-immune-from-cyber-threats.html/

Thompson, E. C. (2018). Cybersecurity incident response: How to contain, eradicate and recover from incidents. *Apress*.

Ursillo, S. & Arnold, C. (2023). Cybersecurity is critical for all organisations– large and small. Retrieved from https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organisations-large-and-small

Warrillow, N. (2024). Cyber attacks are on the increase and no organisation is immune. Retrieved from https://www.scotsman.com/news/opinion/columnists/cyber-attacks-are-on-the-increase-and-no-organisation-is-immune-nick-warrillow-4604733

Wilkinson, I. (2023). What is the UN cybercrime treaty and why does it matter? Retrieved from https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter/

Yasar, K. (2023). Firewall. Retrieved from https://www.techtarget.com/searchsecurity/definition/firewall

Yin, R. (1984). *Case study research*. Beverly Hills: Sage Publications