Cybersecurity Threats to Office Managers in Public Organizations in Anambra State

Volume 1
Number 1
June 2025

Paul-Mgbeafulike, V.S. PhD
Department of Business Education
Nnamdi Azikiwe University, Awka, Anambra State
vs.paul-mgbeafulike@unizik.edu.ng

Ikpeama, Frednora Unchenna, PhD
Department of Business Education
Nnamdi Azikiwe University, Awka, Anambra State
fu.ikpeama@unizik.edu.ng

Udeze, Emmanuel Chukwudile
Department of Business Education
Nnamdi Azikiwe University, Awka, Anambra State

ABSTRACT

The study examined Cybersecurity threats to office managers in public organizations in Anambra State, three purposes of the study and corresponding research questions guided the study. Descriptive survey design was used for the study. The population of the study comprised of all the 298 office managers from all the government ministries and departments. The census method was used hence there was no sampling. The instrument for the study was Cyber Security Threats to Performance of Office Managers (CSTPOM) which was designed by the researchers to elicit information from the respondents. The instrument was validated by three experts. The reliability of the instrument was ascertained through its administration to twenty office managers in Enugu State and the test was repeated on the same group after two weeks interval, The results of the tests were correlated using Pearson Product Moment co-efficient and it yielded a coefficient of 0.81, 0.77 and 0.75 for the three clusters respectively. Mean and standard deviation were used to analyze the data collected. The results show that phishing attacks, ransomware, malware and viruses, unsecured Wi-Fi Networks, and weak password among others are some of the cybersecurity threats affecting performance of office managers. The study recommended among others that Stakeholders in public organizations should procure and install systems that are useful in protecting computer systems against cybersecurity threats.

Keywords: Cybersecurity threats, office managers, public organization.

Corresponding Author's name and email address: Paul-Mgbeafulike V.S. PhD and ***vs.paul-mgbeafulike@unizik.edu.ng***

INTRODUCTION

In this digital era, organizations across the globe are embracing technologies for enhancing efficiency, improving service delivery and effective storage of information. With this development, reliance on digital systems is seemingly one of the factors leading to the exposure of organizations to cyber security threats Adegbite and Ogunleye, (2021). Tran et al (2024), states that cyber threats are posing significant risks to effective use of

technologies in organizations, and this is negatively affecting the office operations in this digital era. Mohurle, and Patil (2017) views cybercrime as the misuse of information and communication technologies for crime or other illegal purposes. This situation is caused by advances in technology where individuals now have access to diverse technologies and some are using them to perpetrate varying crimes. Cybercrime has increased vulnerability of nations and security attention has changed from physical attacks to attacks using technologies (Kumar et al 2021).

These technological attacks have caused a lot of socio-political and economic problems across the globe. Sharma and Gupta (2022) laments that cybercrimes have led to business shutdown as cybercriminals use different strategies in stealing funds from different businesses. Igbuzo (2014) explained that many businesses in Nigeria are no more operating effectively as cybercriminals have fraudulently siphoned their business resources. It is no more news that organizations continually lose millions of naira to cybercriminals, and this negatively affects the socio-economic development of the country. Smith, (2020), listed some of the cybercrimes to include email compromise, social media account hijack, advanced fee fraud, Ponzi schemes, distributed denial of service to mention but a few.

According to Smith, (2020), an increase in different cybercriminal activities could be linked to increased and easy access to cyberspace. In contemporary society, both young and old are having access to cyberspace, which has made many users start using it for illegal activities. Tetrick et al (2021), noted that number of cyber criminals is on the increase because there is increase access to devices that could be used to carryout illegal or illicit activities. Individuals now use the computer, point of sale (POS), the internet and other devices to commit illegal acts. These crimes could be committed against individuals, businesses, organizations and governments can have serious consequences. Yaga et al (2019). explained that cybercrime is mostly initiated through the introduction of viruses, defacement, hacking among others. Cybercrimes could also be linked to property theft, fiscal money, and impersonation among others. All these are against the effectiveness and efficiency of organizations thereby necessitating the need for cyber security. Cyber security could be described as efforts put in place for safeguarding using information and communication technology-based activities ensuring that they don't have any negative effects on the users. According to Rid and Buchanan (2025), Cyber security is the process of safeguarding against threats emanating from the use of the internet. With the increasing rate of cybercrimes, organizations seem to have made efforts towards protecting their data in the digital environment from attack by other internet users. Since insecurity in organizations are no longer restricted to physical based, organizations are beginning to wage digital wars against cybercriminals. These cyber criminals cause individuals, organizations and governments to experience losses in properties, cash and collapse of important resources (Johnson 2021). In this regard, developing strategies towards winning war against varying attacks and crimes is becoming one of the priorities of different organizations.

Identifying and responding to threats that could compromise data that are stored and disseminated through the system will help in enhancing operations of an organization. The main aim of cybersecurity is to protect information and data from been disclosed to unauthorized users to avoid data modification which can affect operations of the authorized users. Kumar et al (2021), notes that cybersecurity integrates different plans and strategies aimed at ensuring that users of digital environment achieve confidentiality, integrity and

constant availability of their information without modifications from unauthorized users. Cybersecurity consists of processes and strategies employed to block unauthorized entry or damage to computers, software, networks and information by criminals. This effort protects organization's data against attacks and helps them to operate efficiently. Cybersecurity is said to be achieved when information and data of an authorized user is protected against attacks and criminal activities. Adegbite (2021) disclosed that cybercriminals usually take advantage of human errors such as not updating their software, clicking on malicious links and creating simple passwords to obtain access to information within a digital environment. This calls for carefulness by all internet users as cyber criminals seem to be improving their ill skills to frequently take advantage of any error from the authorized user. Cybercriminals are constantly looking for slight errors from any internet user so that they will execute their illegal or illicit plans. This, however, makes it imperative for all internet users to always initiate strategies for protecting their computers, software, networks and data from attacks and criminal activities. Inability of users to pay attention exposes them to cybersecurity threats.

One of the major concerns of the users of the digital environment is the increasing rates of cyber security threats. According to Aljawarneh, and Yassein, (2020), organizations and other internet users are frequently exposed to cybersecurity threat due to their reliance on technologies and other digital resources for their operations. Those engaged in cybercrimes understood that important information about organizations is stored in their database thereby improving their ill-skills for easy access to such database. Bennett and Brassard, (2017), observes that increased cybersecurity threats could be attributed to unpreparedness of many internet users to protect and wage war against cybercrimes and attacks. This, however, makes the office managers and their workers vulnerable to the activities of cybercriminals who are constantly monitoring cyberspace to discover errors from the users. Mell, Grance, and Kent (2021), report an increase in cybersecurity threats because of aggressive use of information and communication technologies and growth in the number and diversity of cybersecurity launchers. McAfee also disclosed that availability of tools, expertise and anonymous payment systems has encouraged the growth of cybersecurity threats across the globe. The activities of criminals or hackers that pose cybersecurity threats have made it imperative for office managers to fight towards protecting organization's resources against attacks.

As the definition of office vary according to organizations, same as that of office manager. In some organizations, office managers are seen as those in the administration carder, those possessing special skills required for effective operations within an organization. In other organizations, office managers are seen as those who keep and safeguard information about the organization. Be that as it may, office managers are very important in every organization despite the roles assigned to them. Office managers are pivots of every organization as they are in control of all information used in such an organization. Burns, Roberts, and Hansen, (2020), opine that office managers are also administrators that are responsible for different tasks as regards administration of an organization. Office managers are not only in charge of administrative responsibilities but are also responsible for critical operational functions of any organization. An office manager is responsible for the organization of the office, guiding and controlling activities of office personnel to achieve the organizational goals. Since office managers are most often referred

to as secretaries, their responsibilities include management of correspondence, records and other information within an organization. Henry (20218) opines that office managers are responsible for building a healthy work environment, management and supervision of the entire workspace with the aim of ensuring the smooth running of offices activities and procuring office technologies. Usage of different technologies could lead to delivery of office duties without hitches except nascent cybersecurity threats. In all these cyber-attacks, office managers are usually affected as they are responsible for management of all the office equipment and technologies available or using the office. This makes it imperative to study the impact of cyber security threats on office managers in public organizations.

Statement of the Problem

In this modern digital era, cybersecurity threats have emerged as one of the major concerns of public organizations globally. The roles of office managers in this critical era are pertinent to protect data and other crucial information of public organizations against attacks from cybercriminals. Office managers play crucial roles in ensuring integrity of information within an organization and as well ensure the smooth functioning of administrative operations, which are increasingly dependent on digital platforms. However, the continuous rise in cyber threats is posing significant risks to the efficiency and effectiveness of these office managers. Despite the efforts of managers in public organizations to ensure the implementation of cybersecurity policies, many office managers seem to lack adequate training and awareness regarding the best cybersecurity practices. This gap possibly exposes public organizations to potential security breaches, financial losses, and reputational damage. The increasing reliance on cloud-based systems and remote work arrangements has further amplified cybersecurity vulnerabilities, requiring office managers to adapt to new security challenges. This study therefore was to find out the impact of cybersecurity threats on office managers in public organizations. Specifically, the study sought to:

1. Identify cybersecurity threats affecting the operations of office managers in public organizations
2. Find out the level of cybersecurity measures existing in public organizations
3. Find out the challenges encountered in enforcing cybersecurity policies by office managers in public organizations

Research Questions

The following research questions guided the study:

1. What are the cybersecurity threats affecting the operations of office managers in public organizations?
2. What is the level of cybersecurity measures existing in public organizations?
3. What are the challenges encountered in enforcing cybersecurity policies by office managers in public organizations?

METHODS

The descriptive survey design was used for this study. Descriptive survey design is the type of design which aimed at collecting data and describing it in a systematic manner, the characteristics features or facts about a given population is considered appropriate for the study. The State has Awka as its capital and has 21 local government areas. These local government areas are Aguata, Anambra East, Anambra West, Anaocha, Awka North, Awka South, Ayamelum, Dunukofia, Ekwusigo, Idemili North, Idemili South, Ihiala, Njikoka,

Nnewi North, Nnewi South, Ogbaru, Onitsha North, Onitsha South, Orumba North, Orumba South, and Oyi.

The population was 298 office managers in Anambra State civil service. The population of the study covered all the office managers from all the government ministries and departments in Anambra State. There was no sampling hence census method was used because the number was manageable for this study**.**

The instrument for this study was Cyber Security Threats on Performance of Office Managers (CSTPOMs). The questionnaire was in two sections 'A and B". part "A" was based on demographic data of the respondents while sections "B" has three clusters contained the information on the research questions for the study. The questionnaire was a four-point rating scale; strongly agree (SA), Agree (A), Strongly Disagree (SD), and Disagree (D).

The instrument for data collection was face validated by three experts. A pilot study was carried out using test-retest method. The researchers administered the instrument to twenty office managers in Enugu State and the test was repeated on the same group after two weeks interval. The results of the two tests were correlated using Pearson Product Moment Co-Efficient and it yielded a coefficient of 0.81, 0.77 and 0.75 for the three clusters. Direct delivery method was used in which case the instrument was administered and collected on the spot by the researchers and their five research assistants to avoid high incidence of instrument mortality. Hence, a total of two hundred and ninety-eight (298) copies of the questionnaires administered were as well recovered.

Mean ($\bar{x}$) and standard deviation was used to analyze the research questions. A criterion Mean of 2.5 was generated from the rating scale to help interpret the analysis, any item with mean score of 2.5 and above was agreed, while the one with less than 2.5 was disagreed.

RESEARCH RESULTS

The outcomes of the data analysis are presented according to the research questions posed and hypotheses tested.

Research Question One

What are the cybersecurity threats affecting the operations of office managers in public organizations?

Table 1

Cybersecurity threats affecting the operations of office managers in public organization

S/N	Cybersecurity threats affecting the operations of office managers	Mean	SD	Decision
1.	Phishing Attacks	3.46	0.53	Agreed
2.	Ransomware	3.28	0.99	Agreed
3.	Malware and Viruses	3.51	0.53	Agreed
4.	Insider Threats	2.82	1.03	Agreed
5.	Social Engineering	3.38	1.07	Agreed
6.	Unsecured Wi-Fi Networks	3.24	0.58	Agreed
7.	Weak Password Practices	3.48	0.85	Agreed
8.	Outdated Software and Systems	3.45	0.91	Agreed
9.	Denial of Service (DoS) Attacks	3.0	0.77	Agreed
10.	Data Breaches	2.84	0.58	Agreed
	Grand	3.25	0.78	Agreed

From table 1, shows that all ten items have positive responses on the cybersecurity threats

affecting the operations of office managers in public organizations in Anambra State. The detailed result shows that Phishing Attacks, Ransomware, Malware and Viruses, Insider Threats, Social Engineering, Unsecured Wi-Fi Networks, Weak Password Practices, Outdated Software, Denial of Service (DoS) Attacks and Data Breaches are cybersecurity threats affecting the operations of office managers in public organizations.

Research Question Two

What is the level of cybersecurity measures existing in public organizations?

Table 2

Level of cybersecurity measures existing in public organizations

S/N	Cybersecurity measures existing in public organizations	Mean	SD	DECISION
11	Use of antivirus on all official computers	2.30	0.55	Not Agreed
12	Use of anti-malware software on all official computers	2.52	0.61	Agreed
13	Use of automatic software updates are enabled for operating systems	2.88	0.46	Agreed
14	Use of centralized firewall protection in organization's network	2.63	0.50	Agreed
15	Use of email filtering systems in detecting and blocking phishing attempts	2.22	0.51	Not Agreed
16	Use of data encryption for storing information	2.15	0.47	Not Agreed
17	Use of data encryption for transmitting sensitive information	2.39	0.50	Not Agreed
18	Requirement of unique usernames and passwords for all employees to access systems	2.97	0.49	Agreed
19	Implementation of multi-factor authentication for systems	2.46	0.70	Not Agreed
20	Implementation of role-based access controls to limit data access based on staff roles	2.59	0.48	Agreed
21	Use of endpoint detection and response systems for threat monitoring	2.42	0.63	Not Agreed
22	Regular conduct of vulnerability scans on IT systems	2.69	0.45	Agreed
23	Training of employees on how to identify cybersecurity threats	2.71	0.51	Agreed
24	Training of employees on how to avoid cybersecurity threats	2.64	0.49	Agreed
	Grand	**2.54**	**0.53**	**Agreed**

Table 2 presents the analysis of responses on the level of cybersecurity measures existing in public organizations in Anambra State. It could be seen that items, use of anti-malware software on all official computers, Use of automatic software updates are enabled for operating systems, Use of centralized firewall protection in organization's network, requirement of unique usernames and passwords for all employees to access systems, implementation of role-based access controls to limit data access based on staff roles, regular conduct of vulnerability scans on IT systems, Training of employees on how to identify cybersecurity threats, and training of employees on how to avoid cybersecurity threats were agreed to by the respondents as they were rated above 2.50. while items statement of use of antivirus on all official computers, use of email filtering systems in detecting and blocking phishing attempts, use of data encryption

forstoring information, use of data encryption for transmitting sensitive information, implementation of multi-factor authentication for systems and use of endpoint detection and response systems for threat monitoring were rated below 2.50 implying that they disagreed with the items. The grand mean of 2.54 shows that the responds agreed that there are cybersecurity measures existing in public organizations in Anambra State.

Research Question three

What are the challenges encountered in enforcing cybersecurity policies by office managers in public organizations?

Table 3

Challenges encountered in enforcing cybersecurity policies by office managers in public organizations

S/N	Item	Mean	SD	Decision
25	Cybersecurity roles and responsibilities for office managers in your organization are not clearly defined	3.41	0.98	Agreed
26	Lack of awareness among offices in enforcing cybersecurity policies	3.72	0.65	Agreed
27	Limited training for office managers on emerging cybersecurity threats	3.65	0.88	Agreed
28	Inadequate funding hinders ability of office managers to implement cybersecurity measures effectively	3.33	1.07	Agreed
29	Cybersecurity infrastructure available in public organizations are outdated	3.51	0.84	Agreed
30	Cybersecurity policies in public organizations are complex	3.68	0.77	Agreed
31	Resistance from employees when enforcing cybersecurity protocols	3.24	0.99	Agreed
32	Inability of office managers in keeping up with constantly evolving digital threats	3.59	0.81	Agreed
	Grand	**3.13**	**0.78**	**Agreed**

From the table 3, all the items were rated above 2.5 showing that respondents agreed that the items are the challenges encountered in enforcing cybersecurity policies and managing digital security threats by office managers in public organizations**.**

DISCUSSION

Result of the analysis shows that cybersecurity threats affect the operations of office managers in public organizations in Anambra State. The detailed analysis shows that Phishing Attacks, Ransomware, Malware and Viruses, Insider Threats, Social Engineering, Unsecured Wi-Fi Networks, Weak Password Practices, Outdated Software, Denial of Service (DoS) attacks and Data Breaches are cybersecurity threats affecting the operations of office managers in public organizations. These findings are in line with the study conducted by Williams and Brown (2019), the researchers found that there are different types and degrees of cybersecurity threats that are affecting effective use of information and communication technologies. More so, Chandola et al (2021) notes that despite the existence of different cybersecurity threats, use of technologies is on the increase making it pertinent for organizations to constantly seek for ways of mitigating them. With existence of these threats, it is obvious that cyber security incidents are expected to be occurring in public organizations and office managers who are usually in charge of technologies in the office are largely affected.

The analysis of responses on level of cybersecurity measures existing in public organizations. Items statements of use of anti-malware software on all official computers, use of automatic software updates are enabled for operating systems, use of centralized firewall protection in organization's network, requirement of unique usernames and passwords for all employees to access systems, implementation of role-based access controls to limit data access based on staff roles, regular conduct of vulnerability scans on IT systems, training of employees on how to identify cybersecurity threats, and training of employees on how to avoid cybersecurity threats were agreed to by the respondents as they were rated above 2.50. while items statement of use of antivirus on all official computers, use of email filtering systems in detecting and blocking phishing attempts, use of data encryptionforstoring information, use of data encryption for transmitting sensitive information, impl ementation of multi-factor authentication for systems and use of endpoint detection and response systems for threat monitoring were rated below 2.50 implying that they disagreed with the items. The grand mean of 2.54 shows that the responds agreed that there are cybersecurity measures existing in public organizations in Anambra State. This implies that the respondents agreed that use of anti-malware software on all official computers, use of automatic software updates are enabled for operating systems, use of centralized firewall protection in organization's network, Requirement of unique usernames and passwords for all employees to access systems among others are cybersecurity measures existing in public organizations. On the other hand, the respondents disagreed that use of antivirus on all official computers, use of email filtering systems in detecting and blocking phishing attempts, use of data encryption for storing information, use of data encryption for transmitting sensitive information, implementation of multi-factor authentication for systems and use of endpoint detection are cybersecurity measures existing in public organizations. Aljawarneh and Yassein (2020) posited that increasing rise of cyber security has led organizations into adopting different measures to protect their systems.

The result shows that respondents agreed that all the items are challenges encountered in enforcing cybersecurity policies and managing digital security threats by office managers in public organizations**.** Which are Cybersecurity roles and responsibilities for office managers in your organization are not clearly defined, Lack of awareness among office in enforcing cybersecurity policies, Limited training for office managers on emerging cybersecurity threats, inadequate funding hinders ability of office managers to implement cybersecurity measures effectively among. Smith, Jones and Wagner (2020) in their studies found that though cybersecurity is innovative, implementation of policies and its management comes with different challenges. In this light, office managers in public organizations are sometimes handicapped in ensuring effective enforcement of cybersecurity policies and managing, and this affects their operations in the organizations.

Conclusion

This study highlighted the impact of cybersecurity threats on office managers in public organizations in Anambra State. The findings showed different cybersecurity threats, how they affect the operations of office managers, measures put in place by organizations and challenges to enforcement of cybersecurity policies by office managers in public organizations. Considering the crucial roles of office managers in organizations especially on information management, it is imperative for them to always be prepared against cybersecurity incidents. Their preparation will help in safeguarding information in the organization as they will be able to respond effectively to cybersecurity indicates thereby improving their productivity.

Recommendations

1. Stakeholders in public organizations should procure and install systems and applications that are useful in protecting computer systems from cybersecurity threats.
2. Government at all levels should initiate efforts towards improving on the existing cybersecurity measures and as well initiate new policies in cybersecurity and digital security management.

3. Managers of public organizations should train and retrain office managers on cybersecurity skills, policies and management of digital security threats.

REFERENCES

Adegbite, J., & Ogunleye, T. (2021). *Cybersecurity awareness and management efficiency in Nigerian public institutions*. African Journal of Public Administration, 10(2), 45-60.

Aljawarneh, S., & Yassein, M. (2020). Cybersecurity challenges in public sector organizations. *Journal of Information Security, 8*(3), 45-62.

Bennett, C., & Brassard, G. (2017). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*.

Chandola, V., Banerjee, A., & Kumar, V. (2021). AI-driven cybersecurity solutions: A review. *IEEE Transactions on Information Forensics and Security*, 16, 1523-1542.

Aljawarneh, S., & Yassein, M. (2020). Cybersecurity challenges in public sector organizations. *Journal of Information Security, 8*(3), 45-62.

Henry, A. (2018). Public administration and public affairs. New York: Routledge

Igbuzor, O. (2014), "Public Policy and Poverty Eradication in Nigeria" in Alternative Poverty

Johnson, P. (2021). *Cybersecurity Stress in the Workplace: How Managers Cope*. *Journal of Cybersecurity Studies, 7(2), 45-58.*

Kumar, P., Sachdeva, M., & Kumar, M. (2021). A review on cyber threats and prevention techniques. *Cybersecurity, 4* (1), 1-22.

Kumar, P., Sachdeva, M., & Kumar, M. (2021). A review on cyber threats and prevention techniques. *Cybersecurity*, *4*(1), 1-22.

Mohurle, S., & Patil, M. (2017). A brief study of ransomware: Attacks, prevention, and recovery. *International Journal of Advanced Research in Computer Science, 8*(6), 193-197.

Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. *Journal of Strategic Studies, 38*(1-2), 4-37.

Sharma, P., & Gupta, R. (2022). The importance of firewalls in public sector security. *Cybersecurity Advances*, 10(1), 77-95.

Smith, J. (2020). *Data Protection Regulations and Business Compliance. Business Security Review, 15(4), 112-130.*

Smith, J. (2020). *Data Protection Regulations and Business Compliance. Business Security Review*, *15(4), 112-130.*

Tetrick, S., Robertson, J., & Smith, P. (2021). Cybersecurity training and awareness programs in government agencies. *Government Information Quarterly*, 38(2), 103-121.

Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: An empirical investigation of public servants in Vietnam. *Journal of Asia Business Studies, 18*(6), 1445-1464

Williams, K., & Brown, S. (2019). *Cyber threats and information security policies in U.S. federal agencies. American Journal of Information Security, 7(4), 201-220.*

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *National Institute of Standards and Technology*.

Cite as: Paul-Mgbeafulike, V.S., Ikpeama, F.U. & Udenze, E.C. (2025). Cybersecurity threats to office managers in public organizations in Anambra State. *Journal of Research in Industrial Technology and Educational Studies*, *1*(1), 42-50.