CYBER HYGIENE STRATEGIES: THE KINGPIN OF INFORMATION MANAGEMENT SUCCESS OF DEPOSIT MONEY BANKS IN RIVERS STATE

IKOROMASOMA Emmanuel
Department of Office and Information Management
Faculty of Administration and Management
Rivers State University Port Harcourt
Ikoromasoma.emmauel@ust.edu.ng

ALALIBO Obelem Otonye
Department of Office and Information Management
Faculty of Administration and Management
Rivers State University Port Harcourt
Obelem.alalibo@ust.edu.ng

ABSTRACT

This study examined the correlation between cyber hygiene strategies and information management success of deposit money banks in Rivers State. The study adopted firewall implementation and multifactor verification as dimensions cyber hygiene strategies; while confidentiality and reliability served as the measures of information management success. A Quasi-experimental research design was adopted with a cross-sectional survey approach. The population of the study comprised management staff of 21 deposit money banks operational in Rivers State. Owing to the small population, a census was adopted. Two management staff were studied (branch manager and IT head) from each of the 21 deposit money banks. A total of 42 copies of questionnaire were administered. However, only 38 copies were retrieved and used for the analysis. Data was analyzed using Pearson Product Moment Statistics. The study found that there is a significant positive relationship between hygiene strategy and information management success. Thus, the study concluded that cyber hygiene strategy is an invaluable tool to drive information management success of deposit money banks in Rivers State. The study recommends that management of deposit money banks should encourage firewall implementation and multifactor verification if they seek to improve their information confidentiality and reliability.

Keywords: Cyber hygiene strategies, information management success, multifactor verification, firewall implementation, confidentiality, reliability

INTRODUCTION

Cybercrime has become a thorn posing great challenge in the banking sector in Nigeria and the world large. Considering the deployment of technology in their operations, banks are often faced with online threats and unauthorized access to stakeholders information ranging from transactions, personal details and financial positions amongst others. Deposit money banks have been targets of cybercriminals for some time now. Thus, firms must create cyber-hygiene strategies that could prevent security breaches and stealing of organizations' information assets and customers' personal information (Parker, 2017; Bakzacq & Cavelty, 2016).

Cyber hygiene is a relatively new concept in the information domain which describe practices adopted by individuals and organization to "maintain system health and improve cyber security" with a view to successfully managing information (Tandon, 2019). It involves maintaining proper norms and guidelines in the cyberspace in other to protect data from attackers (Sing et al., 2020). Cyber hygiene can also be seen as efforts made by organizations to protect, maintain and secure devices, networks and data from intruders.

Cyber hygiene is critical to securing information of stakeholders, as human hygiene is critical to our wellbeing. However, the focus of this study is not just on cyber-hygiene strategies, but how it relates to information management success. Therefore, this study view cyber hygiene strategies *as those tools and techniques organizations adopt (firewall installation, multi factor ventilation, encryption and* *data – backups) to ensure the protection and security of data with the aim of successfully managing information.*

It is true that the infiltrations of the internet into our lives and businesses have indeed revolutionized the way we do and approach things. Today, people can stay comfortably at their homes and pay bills, do transactions amounting to huge sums. However, because organizations do not pay critical attention to certain security habits and attitudes, the possibility of these information ending up in the hands of third parties becomes very high; and to avoid this, cyber hygiene becomes critical.

Information management success has gone beyond just identifying, organizing and sharing information, and has included a security aspect. Information cannot be successfully managed if it is not secured. Thus, it will be catastrophic if organizations continue to pay limited attention to the security aspect of managing information. According to Hollander (2019) "the success of organizations depends on the information available to them. This suggests that information is critical to the success of every organization and for organizations to succeed; they must learn to effectively manage their information and that of their stakeholders.

Therefore, it is pertinent to embrace cyber hygiene as the kingpin of information management success. It is on this note that this study opts to examine the correlation between cyber hygiene strategies and information management success in deposit money banks in Rivers State. The study adopted firewall implementation and multifactor verification as dimensions of cyber hygiene. Information management success is represented by confidentiality and reliability.

Consequently, the study formulated the following null hypotheses:
Ho$_1$: Firewall implementation has no significant correlation with information confidentiality.
Ho$_2$: Firewall implementation has no significant correlation with information reliability.
Ho$_3$: Multifactor verification has no significant correlation with information confidentiality.
Ho$_4$: Multifactor verification has no significant correlation with information reliability.

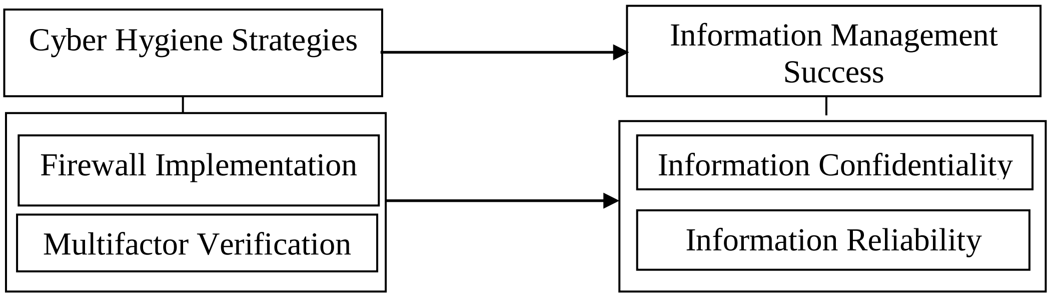

Fig 1: Conceptual framework of relationship between cyber hygiene strategies and information management success

Source: Researchers Conceptualization from review of literature (2024).

CYBER HYGIENE STRATEGIES

There are several attempts to define cyber hygiene. According to Kickpatrick (2015) cyber hygiene is implementing and enforcing data security and privacy policies, procedures, and controls to help minimize potential damages and reduce the chances of data security breach. Considering the challenges posed by cyber hackers, it is imperative to create good hygiene practices that would be carried out routinely to avert or combat threats from hackers. It should be noted that an organization without commendable cyber hygiene practices would end up inviting hackers or malicious insiders to feast on their valued assets: information (Kerfoort, 2012).

Human hygiene is critical to health and wellbeing. Imagine the impact of not brushing our teeth, cutting our nails, or even bathing for days on our health. The same thing is applicable to cyber hygiene, when organizations fail to create good policies that support the documentation of devices, software, and hardware and ensure regular updates. When they fail to orientate staff on need to maintain cyber hygiene and also educate customers on the possible threats of not routinely updating and securing their systems.

Seidenberger (2016), Long (2013), Aloul (2012) and Pike (2011) agree that end users are frequently the weakest link in cyber security. To crown their views, Talib et al. (2019) state that this is especially true within personal computing environments, in which they are the target of 95% of the attacks. This is probably because home and personal computing devices are not protected by information security staff, which keep hardware and software up to date (Anderson & Agarwal, 2010).

Thus, there is need for organizations and their employees to practice cyber hygiene practices. Studies (Almeida et al., 2017; Konieczny, 2015) suggest that cyber hygiene promote safe behaviors and protect against threats. According to O'Connell (2012), good cyber hygiene is "an essential step in maintaining a good cyber defense by applying best practices and educating everyone legitimately using the Internet on good network hygiene.

The number of cyber hygiene practices or strategies a firm can adopt is limited only by the creativity of its leaders. There are as many cyber hygiene strategies as situations and available resources may dictate. In this study however, we adopt firewall implementation and multifactor verification as dimensions of cyber hygiene strategies.

Firewall implementation

Firewall is a piece of software or hardware that allows only authorized access and blocks unauthorized access to network elements or applications. According to Mahmoud (2004) firewalls are computer security systems that protect your office and home networks from intruders, hackers and malicious codes. Security is a critical part of every aspect of our lives whether online or offline, but the focus here is online. And one of the many ways to keep an organization's internal and external networks secured is the implementation of firewalls.

Firewalls are generally configured to secure against unauthenticated intuitive logins from third parties (Kaplesh & Goel, 2019). Usually firewall allows only specified traffic which can be inspected based on IP address, port status, target application, direction of flow of traffic or URL (Kantarcioglu et al., 2004). Extracting from these definitions, this study defined *firewalls as computer security that is a software or a hardware designed for the purpose of blocking unauthenticated access to a computer network.*

Firewalls are key components in the case of internet security, and it has been extensively deployed in most enterprises. According to Tharaka et al. (2016), organizations encourage the implementation of "firewalls that are complex as it may block traffic from outside to within, yet allow users within to communicate a little more freely with the outside". This is to say, when firewall is utilized, security networks and businesses become secured (Kaplesh & Goel, 2019). The implementation of firewall stops other users who may try to connect without permission (Sheth & Thakker, 2011); hence, provide security for data and devices (Nabi et al., 2022).

Multifactor Verification

Despite the growing number of innovative ways to authenticate users, password-based authentication is still one of the most popular methods (Shen et al., 2016). Passwords can easily be memorized and users are able to use them in their daily lives at no cost (Shen et al., 2016). However, passwords can be forgotten (Nicholson et al., 2013). Hence, different methods of authentication have been introduced in the form of biological and graphical passwords. This study defined multifactor verification *as a means of securing personal information with the use of a multiple stage authentication methods with a view to restrict unauthorized access to data*.

Dayaanaym et al. (2009) state that most solutions for today's electronic authentication are the use of username and password. This is to show how imperative a password is to the concept "authentication". However, as good as having a password is, it also pose a big problem when it is taken for granted as it happens to be one of the vulnerability internet attackers look out for before hijacking a system. So, creating a strong password is sacrosanct to cyber hygiene. It is in fact, the first step to protect organizational and customers' online activities.

Today, there are traditional and new threats that make single authentication less reliable. Studies show that multifactor verification provides one of the crucial features of network security. However, it is appalling that some organizations and customers make use of mere conventional passwords such as; 123456, abcdef and some others use their first or last name as their passwords which is often predictive in nature and as such make them vulnerable to potential hackers.

Florence and Herley (2007) found out that nearly half a million internet users use only lower case password. Cone et al. (2006) posit that internet users put security at risk when they select weak passwords or leave their computers logged in. Also, it has been shown that using one password for up to four different sites is dangerous. Thus, organizations and customers must change their password and also avoid the possibility of having to share their passwords with others.

Passwords should be complex but memorable. Dasgupta et al. (2016) states that multifactor authentication enhance security of different application and websites. There is no one best way to creating a password, but one could try to make the password strong by enabling multifactor verification. Cambel and Bryant (2004) found that personal computers can give approximately 80% of common passwords in a week.

INFORMATION MANAGEMENT SUCCESS

Information management is the accumulation and direction of information from one or many reference and the arrangement of that information to those who need it (Robertson, 2005). Information management is conceived to include an endless phase of narrowly connected actions such as identification of informational requirements, procurement and design of information, examination and analysis of information, business and storage of information, information entree and spreading also information procedure (Henczel, 2000; Robertson, 2005; Ravi, 2011).

Maceviciute and Wilson (2002) states that information management entails evolving and applying information procedure and approach, data formation and supervision, processing, storage and information transfer; and information practice. These views of information management are silent on the security aspect of managing information. We therefore argue that they are deficient, as one cannot really manage information successfully without considering information security.

Therefore, this study conceive information management success *as the identification, organization, analyzing, protection, storing and dissemination of this information for effective decision making in an organization.* Information management success is an obligation on the shoulders of management and for one to say information is managed successfully; such information should be reliable and confidential. Reddy et al. (2009) posits that such information should be able to influence transactions and other decisions.

Confidentiality

Confidentiality of information deals with the protection of data from malicious insiders and unauthorized outsiders. The survival of firms depend on their information assets. Hence, firms protect sensitive information from getting into wrong hands. Therefore, the need to invest in cyber hygiene to maintain information confidentiality cannot be overemphasized. According to O'Brien and Yasnoff (1999), confidentiality is defined as the assurance that information about identifiable persons, the rise of which would constitute an invasion of privacy for any person, is not disclosed without consent, except as allowed by law. The breach of stakeholder's confidential data may have the potential to harm them (Blightman et al., 2014).

In this study confidentiality is defined as *non-disclosure and trustworthiness of information related to an organization or individual.* Confidential information includes any information which is not publicly known. This cuts across information related to business, finance, transaction or other affairs of a company or a person. Confidentiality is a set of rules that limits access or places restrictions on the use of certain types of information. It is usually executed through confidentiality agreements and policies. According to Starchin et al. (2019) and de Sousa Costa and de Castro Ruivo (2020), confidentiality is the restriction of access to personal information from an authorized persons and processes at authorized times and in authorized manner. When information is successfully managed, confidentiality is assured.

Reliability

Reliability of information means that a piece information is consistent with known facts, and does not possess contradicting details, either in itself or with related information. Information reliability is one of the parameters of information management success. This is because when information is managed successfully, reliability is most likely to be assured. In today's business world information availability is no longer the problem but reliability of such information remain a major concern considering the continue attacks by intruders in our cyber space where this information is housed.

According to Kazimi (2021), reliability of information in the global space is one of the most important problems faced. Furthermore, this raises issues such as, the accuracy of the information obtained, the accuracy of the source of the information and the harmfulness of the information. The problem of determining the reliability of information on the Internet has become increasingly important as more and more people get their information from the Internet. Therein, we define information reliability *as consistency, justification and accuracy of information such that an organization can bank on it*.

METHODOLOGY

This study adopted a quasi-experimental research design with a cross-sectional survey approach. The population of the study comprised management staff of 21 deposit money banks operating in Rivers State. Considering the limited number of the population, a census was adopted. Two management staff were studied (branch manager and IT head) from each of the 21 deposit money banks, making the sample size equal to 42 management staff. Data was collected via self-constructed questionnaire and data collected were analyzed with Pearson Product Moment Correlation Statistics. 42 copies of questionnaire were administered. However, only 38 copies were retrieved and used for analysis. Below is the Pearson's product moment correlation co-efficient formula.

Table 1: Correlation between Multifactor Verification and Confidentiality

		Multifactor Verification	Confidentiality
Multifactor Verification	Pearson Correlation	1	.922**
	Sig. (2-tailed)		.000
	N	38	38
Confidentiality	Pearson Correlation	.922**	1
	Sig. (2-tailed)	.000	
	N	38	38

**. Correlation is significant at the 0.05 level (2-tailed).

Source: SPSS Version 22 Output, 2024

Table 1 indicates the Pearson product-moment order correlation coefficient (r) between multifactor verification and confidentiality. It was observed that multifactor verification has very strong positive and statistically significant correlation with confidentiality (r = 0.922, p = 0.000 < 0.05). This suggests that deposit money banks in Rivers State can improve the information confidentiality if they implement multifactor verification.

Table 2: Correlations between Multifactor Verification and Reliability

		Multifactor Verification	Reliability
Multifactor Verification	Pearson Correlation	1	.922**
	Sig. (2-tailed)		.000
	N	38	38
Reliability	Pearson Correlation	.922**	1
	Sig. (2-tailed)	.000	
	N	38	38

**. Correlation is significant at the 0.05 level (2-tailed).

Source: SPSS Version 22 Output, 2024

Table 2 indicates the Pearson product-moment order correlation coefficient (*r*) between multifactor verification and reliability. It was observed that multifactor verification has very strong positive and statistically significant correlation with confidentiality (*r* = 0.922, p = 0.000 < 0.05). This suggests that deposit money banks in Rivers State can improve the information reliability if they implement multifactor verification.

Table 3: Correlations between Firewall Implementation and Confidentiality

		Firewall Implementation	Confidentiality
Firewall Implementation	Pearson Correlation	1	. 891**
	Sig. (2-tailed)		.000
	N	38	38
Confidentiality	Pearson Correlation	. 891**	1
	Sig. (2-tailed)	.000	
	N	38	38

**. Correlation is significant at the 0.05 level (2-tailed).

Source: SPSS Version 22 Output, 2024

Table 3 indicates the empirical result of Pearson Product-Moment Order Correlation Coefficient (*r*) between firewall implementation and confidentiality. It was observed that firewall implementation has very strong positive and was statistically significant correlation with confidentiality (*r* = 0.891, p = 0.000 < 0.05). This means that implementation of firewalls enhance information confidentiality of deposit money banks in Rivers State.

Table 4: Indicates Correlations Analysis on Firewall Implementation and Reliability

		Firewall Implementation	Reliability
Firewall Implementation	Pearson Correlation	1	.873**
	Sig. (2-tailed)		.000
	N	38	38
Reliability	Pearson Correlation	.873**	1
	Sig. (2-tailed)	.000	
	N	38	38

**. Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS Version 22 Output, 2024

Table 4 indicates the Pearson Product-Moment Order Correlation Coefficient (*r*) between firewall implementation and reliability. It was observed that firewall implementation has very strong positive and statistically significant correlation with reliability (*r* = 0.837, p = 0.000 < 0.05). This indicates that improvement in implementation of firewalls by deposit money banks will result to increased information reliability.

DISCUSSION OF FINDINGS

The findings revealed that there is a significant and positive relationship between cyber hygiene strategies and information management success. The study findings also revealed that there is a significant positive relationship between firewall Implementation and the measures of information management success of deposit money banks. This finding agrees with the assertions of Kaplesh and Goel (2019) firewalls generally are configured to secure against unauthenticated intuitive logins from third party.

The study findings revealed that there is a significant positive relationship between authentication and the measures of information management success of deposit money banks. This finding agrees with the assertions of Dasgupta, Roy and Nag (2016) that what have been declared as password weakness, multi-factor authentication aiming at enhancing the security of different application and website has become more popular.

CONCLUSION AND RECOMMENDATIONS

Based on the data collected and analysis, the study concluded that there is a significant positive relationship between the study variables. Therefore, in managing information, cyber hygiene serves as the kingpin and should be paid considerable attention.. Hence; firewall implementation and multifactor verification positively and significantly relate with information management success expressed in terms of confidentiality and reliability. Therefore, cyber hygiene strategy is an invaluable tool to derive information management success. Based on this conclusion, the study made the following recommendations;

i. Management of deposit money banks should encourage multifactor verification as it a critical tool for information management success which results in confidentiality and reliability of information.
ii. Management of deposit money banks should strengthen firewall implementation as it have been found to address cyber threats and vulnerability which in turn enhances information management success expressed reliability and confidentiality of information.

REFERENCE

Almeida, K., Promise, G., & Landy, K. (2017). Toward principles of cyberspace security. *Cyber Security Policies and Strategies for Cyber Warfare Prevention*, *1*(12), 201.

Aloul, F.A. (2012). The need for effective information security awareness. *J Advance Information Technology, 3*(3), 176-183.

Bakzacq, D., & Cavelty, R. (2016). *Information management in engineering education.* Lehigh University Press.

Blightman, K., Griffiths, S., & Danbury, C. (2014). Patient confidentiality: When can a breach be justified? *Contin Educ Anaesth Critical Care Pain, 83*(1), 99-113.

Campbell, J., & Bryant, K., (2004). Password composition and security: an exploratory study of user practice. *ACIS 2004 Proceedings.* Retrieved from https://aisel. aisnet.org/acis2004/80.

Cone, B. D., Thompson, M. F., Irvine, C. E., Nguyen, T. D. (2006). Cyber security training and awareness through game play. In: *Proceedings of IFIP international information security conference.* 431–436.

Dasgupta, D., Roy, A., & Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication. *Computer Security, 63,* 85–116.

Davaanaym, Y. S., Lee, H. J., Lee, S. G., Lee, B., & Lim, H. T. (2009). A ping pong based one-time-passwords authentication system. Proceedings at *5th International Joint Conference. IEEE Computer Society,* 574–579.

de Sousa Costa, R., de Castro Ruivo, I. (Eds)(2020). *Preliminary remarks and practical insights on how the whistleblower protection directive adopts the GDPR principles*. Annual Privacy Forum, Springer.

Florencio, D., & Herley, C., (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*.

Henczel, L. (2000). A transparent, incremental, concurrent checkpoint mechanism for real-time and interactive applications. *Journal of Information Science and Engineering, 12*(1), 23-32.

Hollander, R. (2019). Competing values in software process improvement: An assumption analysis of cmm from an organizational culture perspective. *Transactions on Engineering Management, 50*(1), 11-24.

Kantarcioglu, J., Jin, O., & Clifton, T. (2004). Mental models of privacy and security. IEEE *Technology and Society Magazine.*

Kaplesh, P., & Goel, A. (2019). Firewall: A study on technology, security and threats. *Pramana Research Journal, 9*(4), 312-323.

Kazimi, P.F. (2021). Dynamic development of information technologies, organization of liberary services using digital space and through social networks. *Asian Journal of Education and Social Studies, 16(*4), 27-32.

Kerfoot, O. (2012). Processes as theory in information systems research, Arlborg, Germany, *International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology.*

Kickpatrick, K. (2015). Cyber security without cyber war. *Journal of Conflict and Security Law, 17*(2), 187–209.

Konieczny, F. (2015). SEADE: Countering the futility of network security. *Air Space Power Journal, 29*(5), 4.

Long, R. M. (2013). *Using phishing to test social engineering awareness of financial employees*. Eastern Washington University. Doctoral dissertation.

Maceviciute, C., & Wilson, T.D. (2004). The development of the information research area. *Information Research, 7*(3).

Mahmoud, M.Y. (2004). *Computer firewalls,* 3-261.

Nabi, A. U., Ahmed, M., & Abro, A. (2022). An overview of firewall types, technologies and functionalities. *Journal of Computing and Related technologies, 3*(1), 1-7.

O'Brien, D.G., & Yasnoff, W.A. (1999). Privacy confidentiality, and security in information systems of state health agencies. *American Journal of Preventive medicine, 16*(4), 3555-358.

O'Connell, P. (2012). Cyber security countermeasures to combat cyber terrorism, *Strategic Intelligence Management*, 234–261.

Parker, E. (2017). An actor-network theory reading of change for children in public care. *British Educational Research Journal, 43,* 151-167. doi:10.1002/berj.3257

Pike, M. (2011). *The magazine for the IT professional. The Charted Institute for IT*. British Computer Society.

Priyadarshini, J., & Cotton, O. (2022). Community-oriented culture and simple organizational structure, *"Organization and Management, 3*(1), 23-32.

Ravi, I. (2011). *Cyber security threats detection in Internet of Things using deep learning approach,* IEEE Access.

Ravi, V. (2011). A two-factor authentication system with QR codes for web and mobile applications. In: Proceedings – 2014 *International Conference on Emerging Security Technologies*, 105–112.

Reddy, S., Srinivasu, R., Rikkula, S.R., & Rao, V.S. (2009). Management information systems to help managers for providing decision making in an organization. *International Journal of Reviews in Computing, 15*, 1-6.

Robertson, N. (2005). *Developing cyber security culture to influence employee behavior: A practice perspective,*

Seidenberger S. (2016). A new role for human resource managers: social engineering defense. *Cornell HR Review.* http://www.digitalcommons.ilr.cornell.edu/chrr/95

Shen, C., Yu, T., Xu, H., Yang, G., Guan, X., (2016). User practice in password security: an empirical study of real-life passwords in the wild. *Computer Security, 61,* 130–141.

Sheth, C., & Thakker, R. (2011). Performance evaluation and comparative analysis of network firewalls. Proceedings at *International Conference and Device and Communication,* (1-5).

Sing, G., Mohanty, T., Swagatika, A. & Kumar, P. (2020). *Developing a management climate culture in which information technology will flourish: How the UK can benefit.*

Starchon, P., & Pikulik, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices-mobile phones. *Procedia Computer Science, 151*, 12-303.

Steifer, F. (2022). *A theory of information technology cultures: magic dragons. Wizards and archetypal patterns.* Unpublished doctoral dissertation.

Talib, S., Clarke, N. L., Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *Proceedings of the International Conference on Availability, Reliability, and Security,* 196–203. doi:10.1109/ARES.2010.27.

Tandon, G. (2019). Cyber security for a smart grid-what about phishing? *Proceedings of innovative smart grid technologies Europe*. doi:10.1109/ISGTEurope.2013.6695407.

Tharaka, S.C., Silva, S., Sharmila, S.U.I., Silver, K.L.D.N., Liyanage, A.A.T.K.K., Amarasinghe, D., & Dhammearatchi (2016). High security firewall: Prevent unauthorized access using firewall technologies. *International Journal of Scientific and Research Publications, 6*(4).