MULTI-FACTOR AUTHENTICATION AND INFORMATION SECURITY OF TELECOMMUNICATION FIRMS IN SOUTH- SOUTH NIGERIA

BROWN Miller Ibiso
Department of Office and Information Management Faculty of Administration and Management, Rivers State University

ABSTRACT

Multi-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of factors (evidence) to an authentication mechanism. The adoption of multi-factor authentication is shaping the lives of individuals and organizations to have a secure data environment, due to the prevalent nature of cyber attacks as well as unauthorized access to information. With cyber crimes on the rise, organizations are encouraged to be proactive by stepping-up their information security with the adoption of multi-factor authentication as a more secure means of information security. Organizations are being urged to adopt multi-factor authentication due to its unique way of safeguarding unauthorized access to information. Bearing in mind that in today's turbulent business world organizations are choosing multi-factor authentication more often, the purpose of this paper was to analyse the very process of multi-factor authentication. The deployment of MFA provides the establishment of unique information security policy for managing a company. Based on the analysis of literature, the author stresses that Multi-factor authentication cannot be ignored if Telecommunication firms in Nigeria wishes to achieve higher optimization and overall efficiency.

Keywords: Multifactor Authentication, Information Security and Telecommunication

INTRODUCTION

Organizations are finally increasing their level of consciousness regarding information security management, due to the relevant nature of organizational information regarding competitiveness and survival in global markets. The importance that has been gained by information security management in enterprises worldwide has been enormous. On one hand, management boards are becoming aware about the need to protect data and information and, on the other hand, cyber attacks are booming, as documented by worldwide cyber security institutions and the level of consciousness about the need to implement countermeasures have comprehensively increased. With society's increasing dependency on information technology (IT), the consequences of security breaches can be extremely grave (Power, 2002). In addition to monetary losses, breaches of information systems can also cause damages to businesses such as disruption of internal processes and communications, the loss of potential sales, loss of competitive advantage, and negative impacts on a company's reputation, goodwill and trust (Bruce, 2003). As a result, information security management (ISM) has become a required function (Filipek, 2007). In many cases, it is impossible or nearly impossible to run a business without the smooth and secure operation of its information systems (Zviran & Haga, 2009).

To protect organizational information assets from both internal and external attacks, many different information security standards and guidelines have been proposed and developed. For example, the generally accepted system security principles (GASSP) is a joint international effort between ten countries to develop a set of rules, practices, and procedures to achieve information integrity, availability, and confidentiality. The Federal Information Processing Standards Publications (FIPs PUBs) provided guidelines that are mandatory for government agencies, but optional for the private sector. The International Organization for Standardization (ISO) 17799 is described as a suitable model for ISM and an appropriate vehicle for addressing ISM issues in organizations (Dhillon & Blackhouse, 2001). Additionally, ISM literature has provided different checklists (Dhillon and Blackhouse, 2001)

and hundreds of “best practices” (Stefanek, 2002) for practitioners to use. Information Security Management relates to the protection of valuable assets against unavailability, loss, misuse, disclosure or damage. In this context, valuable assets are the information recorded on, processed by, stored in, shared by, transmitted from or retrieved from any medium. The information must be protected against harm from threats leading to different types of impacts, such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents, and intentional damage and these measures are adopted by organizations in order to control the level of access to such valuable and sensitive organizational resources.

With the advancements of information technology, most user online access to the online accounts had counted on various online services, which needed to be secured and trusted in a way to prevent the thorny issues of illegal access, identify theft and data breaches. According to O’Leary (2017), the authentication problems were still increasing dramatically due to dynamic threats, the application security statistics reported that 81% hacking breaches of stolen passwords, and 93% financially compromised by criminals. These incidents affected user’s tremendous burdens and insecure accesses the online system. Authentication method was the mandatory factor to address the trustworthiness, to identify user credentials and to restrict illegal and unauthorized access to the system. For instance, authentications through a single factor with user ID and password. If a single factor authentication mechanism failed, the users could not get access to the online systems until a system administrator checked and recovered the actual system. Thus, the single factor authentication was suffering from some significant pitfalls. To improve the single factor authentication issue, authentication through additional factors became paramount for system administrators to enforce data security policies and procedures on all database levels. So that only legitimate users could have right permissions to get access to computing systems.

The use of multiple authentication factors with various weights associated with pre-defined criteria makes it harder for intruders or malicious attackers to gain unauthorized access to the systems. Most authentication systems in use nowadays verify a user's credentials during the login time to the systems. For example, two-factor authentication systems used in different email servers that had been checked for two separate factors at the time of accessing the online services for the first time but did not validate the second time throughout the ongoing session; thus, this scenario could increase the chance of compromising user credentials and the authentication was not verified throughout the ongoing session of any user who opened a back door for hackers to imitate the actual user to login to the systems. In addition, mobile technology continued to increase user's access to online systems. Thus, checking the authenticity of the registered users daily was very important for system administrator to protect sensitive data from tampering or unauthorized attempts. Therefore, the trustworthiness algorithms enhanced the need for system administrator to increase or decrease the resiliency of adaptive multi-factor authentication system. Multi-factor authentication is a more secure authentication that was required and it is one of the methods of authentication technique, which was selected from further criteria selections. This method is used to double check the users' identity prior to accessing the sensitive and confidential data (Centrify). MFA added a layer of security that allows system administrator to link two or more types of authentication to provide better way of authenticating users. By doing this technique, it protected against the compromised data. The most common four types of authentication factors are: the first one is "something the user knows", for example: username, password, PIN or security questions. The second one is "something the user has"

that is the device the user possesses like the Smartphone device or smart card. The third one is "something the user is" that is s a user's physiological traits, for instance, biometrics, fingerprint, retina scans or voice recognition. The last one was "where the user is" that was a user's location, for example IP address to identify the geographic location of the users (Bolle et al., 2004). This paper was designed to theoretically review relevant literature on the relationship between multi-factor authentication and information security of telecommunication firms. In doing so, this reviewer presents an initial step toward an integrated framework of multi-factor authentication, which provides new insights into our understanding of the existing literature as well as a useful guide for future research. A conceptual framework of the relationship between multi-factor authentication and information security is shown in figure 1.

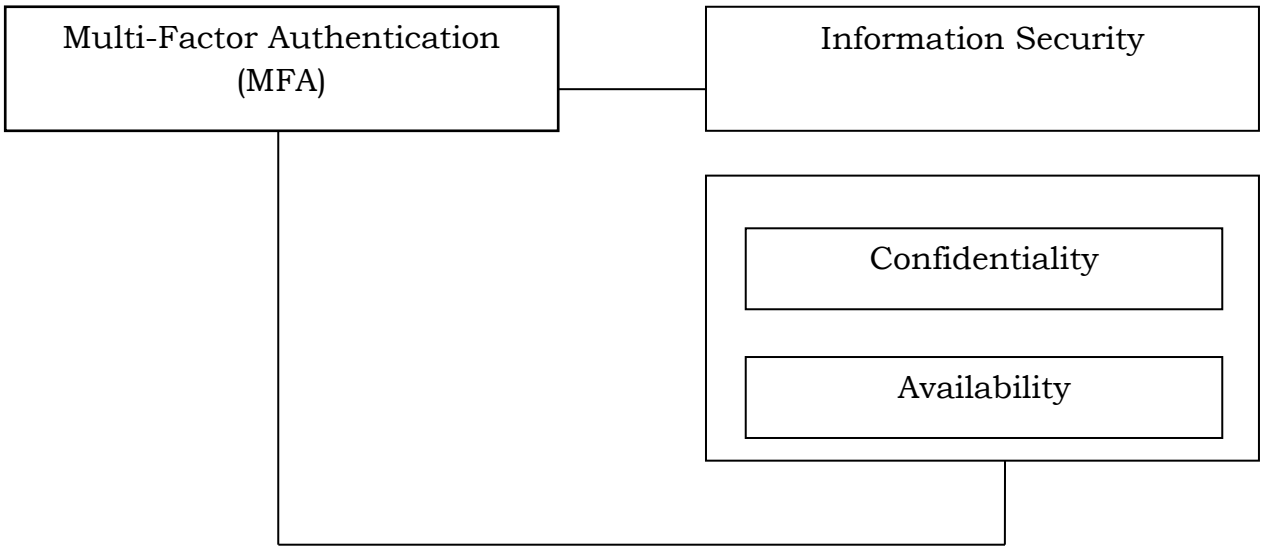

Figure 1: Conceptual Framework for Multi-Factor Authentication and Information Security of Telecommunication Firms in South-South, Nigeria.

Source: Researcher's Desk (2024).

THEORETICAL FRAMEWORK

Resource Based Theory (Jay Barney 1990)

The baseline theory associated with this study is the resource based theory basically because the resource based theory suggests that resources that are valuable, rare, difficult to imitate and nonsubstitutable best position organisations for long-term success. These strategic resources can provide the foundation to develop the organisations' capabilities that can lead to superior performance over time.

CONCEPT OF MULTI-FACTOR AUTHENTICATION

According to Grimes (2021) humans know authentication and have been utilizing it for ages. The simplest and oldest authentication method is personal recognition. If you are going to meet someone, an authentication process will happen during the meeting, by recognizing the

face and accept the person. Moreover, in workplace, if you are waiting for documents, you will accept them based on the signature of approvers on them. Regardless of authentication methods, the result of accepting someone or something is the same. It is basically two ways channel that has two nodes A & B, while B will be challenged to be accepted by A. With the fact that nowadays our life has been changed and full with network and computer and cyber spaces, personal recognition is not valid any more. Authentication methods were evolved to fulfil recent complex life requirements to ensure the availability, confidentiality and integrity of the information.

Nowadays, information is the most important asset in any organization. Therefore, securing the environment and apply the needed controls become a mandatory thing in order to assure business sustainability. Many security companies offer several solutions to secure systems, such as encryption, passwords, certificates and authentication. A new concept rose recently which is Multi Factor Authentication (MFA). Multifactor authentication (MFA) is a security technology used to verify user's identity to access a system or application which requires multiple steps to validate user's credentials. Multifactor authentication combines two or more self-governing credentials: what the user *knows*, such as a password; what the user *has*, such as a security token; and what the user *is*, by using biometric verification methods. The objective of MFA is making it more difficult to compromise the system. In case a hacker knows the credential for a system or application and tried to login, he will be challenged against another factor to satisfy it before successfully login to it.

An authentication method is used with user's credentials to guarantees identity verification. Each additional authentication method in MFA is intended to challenge the user of the system in several ways such a who, or what it says it. Several authentication questions will help complicate hacker's job. A lot of organizations are using MFA, as an example, Google supports different kinds of MFA methods among its services. This eventually will help them to secure their services by challenging attackers to access services or take over user accounts in Google. The importance of MFA is intangible, as it will improve the security for any organizations. It will add additional security layers in applications, services, or systems to require the attacker to give more effort to search for another way to successfully take over the system. In addition, MFA support digital transformation through supporting remote workforce, cloud, and e-commerce. All of them requires secured environment in the current digital era. Moreover, MFA can be vital method to assure the sustainability of online interactions and secured transactions. Simplifying the work is an essential need by users to assure accessing the system easily. As well as application's developers and/or system administrators to entice users to assures providing user friendly environment. However, MFA method will add additional layer and extra step, which will complicate the utilization of any system.

Nature of Information Security

Information security management, according to the International Standards Organization (ISO), is the "protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (ISO-27002, 2005). Information security management, according to the National Institute of Standards and Technology's (NIST*)* Information Security Handbook, involves planning for and implementing a structure as well as the processes that provide for the alignment of information security strategies with business objectives and applicable laws and industry standards (Bowen, Hash, & Wilson, 2006). The ISO Information technology

security techniques; Code of practice for Information Security management (ISO, 2005) argued that information security is becoming increasingly more important for both public and private sector businesses as the interconnection of public and private networks and the sharing of information resources increase the complexity of controlling access and preserving the confidentiality, integrity, and availability of data. Jenkins (2002) noted that information that is lost or stolen often causes financial damage and may tarnish the public image of an organization. Von Solms & Von Solms (2000) believed that securing information is one of the most important aspects in any organization today and that the primary aim of information security is to protect the organization and its assets (such as sensitive information) against attempts of intrusion and corruption.

Confidentiality

According to (Beck et al 2011), confidentiality and privacy refer to how professionals must handle pieces of information gathered during medical care. But confidentiality and privacy is not only limited to information gathered during medical care, it covers every piece of information be it personal or institutional. Hence, necessary effort has to be geared towards the protection and safeguarding of information from being disclosed to unauthorized users. Confidentiality concerns the attitude required of information professionals to handle information resulting from this relationship. The three attributes; secrecy, privacy and confidentiality are professional obligations when handling information. In addition, these three attributes are also rights of users.

Primary health care teams, organizations which also include community health agents, access and handle a lot of information on users. Thus, it is appropriate to discuss how to respect the secrecy and privacy of such information while working in a multidisciplinary team. The exchange of information between users and professionals is, in principle, related to the trust created in their relationship. This relationship depends on the quality of access and how users are received in the service, both marked by the establishment of a relationship based on user embracement, or yet, marked by the absence of such relationship. User embracement is a step of the service "production process". And this process allows the connection between users, professionals and services, leading to the establishment of "accountability" and consequent solution of information production processes. In this user-embracement context, privacy of user information shared among the team is agreed upon as a confidentiality "pact". Therefore, an agreement among team members and users in regard to the handling of secret and private information must begin at the moment of embracement and continue all throughout the period of employment, so as to establish a bond based on ethical precepts of respect to autonomy and to users' uniqueness as well as of adequate information handling. Organizational information contains sensitive information such as patent rights, if revealed to just anyone, competitive advantage can be lost in split seconds to a competitor all because of the disclosure of information to the wrong person. As a result, organizational information has to be protected at all cost, since it is a veritable tool that drives decision making.

Availability

Availability is the "timely, reliable access to data and information services for authorized users" (Schou, 1996). More broadly, availability is about information being accessible as needed, when needed, where needed. The objective of availability is to enable access to authorized information or resources (CEC, 1991). According to Viles & French (1995), most users expect a "100-100 Web: 100 percent availability for all servers and 100 millisecond latency to every server." This expectation is nearly impossible to sustain, given the many

threats to availability. It is reasonably well established that availability has three components: *Reliability*, *Accessibility*, and *Timeliness*. *Reliability* is "the probability of a system performing its purpose adequately for the period of time intended under the operating conditions encountered" (Reibman & Veeraraghavan, 1991). Users do not want to depend upon a system that cannot be trusted to consistently execute their requests. Broadly speaking, *accessibility* is "the degree to which a system is usable by as many people as possible without modification". There are several access control policies, such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC) which are supported with access control services such as Role Based Access Control (RBAC) (Sandu, 1996). *Timeliness* is the responsiveness of a system or resource to a user request. Traditionally IAV has mostly been measured by the amount of time an information resource is either processing or not (uptime and downtime) (Wood, 1995).

MULTI-FACTOR AUTHENTICATION AND INFORMATION SECURITY

The reference research work of this field covered different aspects of multi-factor authentication but the paper did not clarify how such multi-factor authentication is implemented. (Bolle et al, 2004), research provides great work about multi-factor authentication as it describes the essence and need for the adoption of multi-factor authentication by organizations, since the business success of organizations hinges on their ability to successfully protect its most valuable resource from being breached by hackers. The motives for application of multi-factor authentication are the following: An effective cyber security solution, complied with Single Sign-On (SSO) solutions, regulatory compliance, assures consumer identity and provision of more layers of security (Grimes, 2021). Many studies have been conducted worldwide studying multi-factor authentication. (Kim, 2018) conducted a research on the implementing resiliency of adaptive multi-factor authentication systems in St. Cloud State University, Minnesota. From the forgoing discussions and from the review of relevant and empirical literature, it appears that there is a relationship between multi-factor authentication and information security variable and on the strength of the above assertion, the author hypothesizes as thus:

H_{A1}: There is a significant relationship between multi-factor authentication and information security of telecommunication firms in South- South Nigeria.

CONCLUSION

The relevance of multi-factor authentication in influencing information security of telecommunication firms and the Nigerian economy cannot be ignored. An organization whose information/data is protected using multi-factor authentication can bring about increased confidentiality, availability of information and overall administrative efficiency. Accessibility and network security tools are very important aspects of data management activities and the ability to plan and perform proactive man oeuvres is paramount and essential for success of today's businesses. This paper has elaborately discussed the concept of multi-factor authentication and its relationship with its identified attributes, the nature of information security with its measures, the connection between multi-factor authentication and information security. The study theoretically revealed that multi-factor authentication relates with information security; hence the author recommended that Telecommunication Firms in Nigeria should regularly and carefully adopt multi-factor authentication as a more secured means of enhancing overall organizational performance as well as the enhancement of relevant network security processes and tools that protects sensitive business information from being breached by unauthorized or malicious users.

REFERENCES

Beck, J, Mandalia S, Harling G, Santas X, Mosure D, Delay P. (2011). Protecting HIV-Information in Countries Scaling Up HIV Services, *Journal of the International AIDS Society*, 14:6 (http://www. biomedcentral.com/content/pdf/1758-2652-14-6.pdf).

Bolle, R. M., Nunes, S. L, Pankanti, S., Ratha, N. K., Smith, B. A., & Zimmerman, T. G. (2004). "Method for Biometric-based Authentication in Wireless Communication for Access Control". (Publication: US 6819219 BI), 2004

Bowen, P., Hash, J. & Wilson, M. (2006). Information Security Handbook: *A Guide for Managers. National Institute of Standards and Technology publication 800-100*.

Bruce, L. (2003). Information security–key issues and developments", available at: www.pwcglobal. com/jm/images/pdf/Information%20Security%20Risk.pdf (accessed February 2007).

CEC: Commission of the European Communities (1991). *Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria: Version 1.2* Luxembourg: Office for Official Publications of the European Communities.

Dhillon, G. & Blackhouse, J. (2001). "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, (2), 127-53.

Filipek, R. (2007), Information security becomes a business priority", Internal Auditor, Vol. 64 No. 1, p. 18.

Grimes, R. A. (2021). Hacking Multifactor Authentication, John Wiley & Sons Inc.

ISO (2005). Information technology Security techniques: *Code of Practice for Information Security management*. International Standards Organization (ISO) document. Reference number ISO/IEC 27002:2005(E).

Jenkins, G. (2002). Information Systems: *Policies and Procedures Manual.* Paramus, NJ: Prentice Hall

Kim, G. P. (2018). Implementing Resiliency of Adaptive Multi-Factor Authentication Systems. A Starred Paper Submitted to the Graduate Faculty of St. Cloud State University in Partial Fulfilment of the Requirements for the Degree of Master of Science in Information Assurance

O'Leary, R. (2017). It's here: The 2017 White Hat Security Application Security Statistics Report! - White Hat Security. Retrieved October 20, 2017, from https://www.whitehatsec.com/blog/application-security-statistics-report/

Power, R. (2002). CSI/FBI Computer Crime and Security Survey: Computer Security Issues & Trends, 8(1), 1-22.

Reibman, A. L. & Veeraraghavan, M. (1991). Reliability Modeling: An Overview for System Designers *Computer*, 24(4), 49-57.

Sandu, R. (1996). Access control: The neglected frontier. *Proceedings of the First Australasian Conference on Information Security and Privacy*, Australia, 219-227.

Stefanek, G. (2002). Information Security Best Practices 205 Rules, Butterworth-Heinemann, Boston, MA.

Schou, C., Editor (1996). *Information Systems Security Organization (ISSO) Glossary of INFOSEC and INFOSEC related terms,* Vols. 1 & 2. Idaho: Idaho State University.

Viles, C. L. & French, J. C. (1995). Availability and Latency of World Wide Web Information Servers. *Computing Systems*, 8 (1), 61-91.

Von Solms, E. & Von Solms, S.H. (2000). *Information Security Management Through Measurement*. Norwell, MA: Kurwell Academic

Wood, C.C. (1995). Writing Infosec Policies. *Computers & Security, 14*(8), (pp. 667-674).

Zviran, M. & Haga, W. (2009). Password security: an empirical study", *Journal of Management Information Systems*, 4 (15), 161-85.