Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Academic Innovations City University Foundations

Proceedings of the Cyber Secure Nigeria Conference – 2024

Protecting Organisations' Data against Insider Related Breaches

[1]Adeniyi Akanni, [2]Peter Oduroye & [3]Olajide Adegunwa
[1,2,3]Caleb University
Imota, Lagos State, Nigeria
E-mail: adeniyi.akanni@calebuniversity.edu.ng

ABSTRACT

The dependence on computer systems has grown exceedingly much during the obnoxious COVID -19. Afterwards, it has not waned. Many activities and transactions have thus been moved virtual. All sectors also leverage the gains brought about by technology to advance their efficiency. However, the rate of data breaches has also spiked and organisations keep battling to protect of resources. More worrisome is the issue of breaches traceable to have arisen from within the organisation, even after fortifying the network with a firewall, router and other measures against external attacks. This research attempted to proffer a solution to protect organisations' data against insider-related breaches. While cybersecurity is an all-encompassing activity, the research proposed a symmetric encryption. The study revealed that 100% of respondents believed that insider-rated breaches (IRB) would lead to losses. Thus, a solution would be needed to protect against data breaches with a view to minimising losses to organisations.

Keywords: Insider-related breaches, encryption, compromise, security, confidentiality

Proceedings Citation Format
Adeniyi Akanni, Peter Oduroye & Olajide Adegunwa (2024): A Modern Perspective on the Impact of Artificial Intelligence on Cyber Diplomacy. Proceedings of the Cyber Secure Nigeria Conference held at The Ballroom Center, Central Business District, Federal Capital Territory, Abuja, Nigeria - 25th - 26th September, 2024. Pp 175-180. https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/
dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P16

1. INTRODUCTION

Security of resources is always of the utmost importance to organisations. Whatever the nature or set up of an organisation, it is always on the mind of the management to device and design appropriate measures to protect their cyber resources, which include: computer systems, servers, networks, switches, routers, printers, mobile devices, data and lots more.

Appropriate controls are then put in place to give an opinion that such internal workings give some reasonable assurance that threats and vulnerabilities are covered. In some cases, Access Control may be put in place; a maker-checker arrangement, Configuration of a firewall, monitoring suspicious transactions and a host of others. Most times, attention is always drawn to the external attack by the lines of defence put in place, while undermining the insider threats. Since humans play a key role in Information and Communication Technology (ICT), it becomes extremely necessary to consider the aspect of man's involvement in cyber activities to ensure that the security objectives are achieved. Internal collusion or negligence on the part of staff, vendors or contractors can be sources of breaches if adequate controls are not in force. Insiders have unfettered access to sensitive areas that every other stakeholder is restricted from. Data and information can be unduly exposed to an unauthorised person. This might have been unwittingly done. At some other points, a disgruntled staff can also become a sellout. Whichever way, insider-related breaches (IRB) for organisational data must be checked to prevent losses.

Insider-Related Breaches

Health and Human Services (2022) defined insider threats to include individuals who can negatively use privileged information they can access due to access they have because of working for an organisation. Schulze (2024) observed that insider-related vulnerability has increased significantly in 2023. He also noted that the loss as a result of the breach cut across so many key areas such as reputation, brand, data and revenue. Thus, emphasising the need for given security against insider-related threats. Mazzarolo & Jurcut (2019) opined that cybercrimes committed by internal actors can be malicious or due to carelessness. Invariably, no organisation is immune since internal users can be used as conduits or as main actors in such crimes (Whitelaw, 2024).

Today's world has not changed for the better in the area of cyber security breaches, especially from personnel of the organisation who may divulge confidential details for so many reasons ranging from illicit gains to ignorance (Chen et al, 2019). Whichever way, a compromise is established. Many approaches had been sought in the past, including signing the non-disclosure agreement, cyber security awareness training and a host of others. While we agree that cybersecurity should be all-encompassing and that one can complement the other, a symmetric encryption approach is proposed.

Survey

A survey was carried out, and the outcome revealed that the issue of insider-related threats and attacks cut across sectors; anyone from management to operational staff can fall victim, even without suspecting and can lead to a quantum loss depending on the severity.

The figures

a. IRB can occur irrespective of Sector

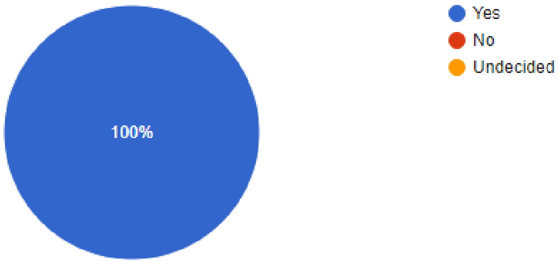

Fig 3: Insider Related Breaches is Sector Independent

Fig. 3 shows that it can occur in any sector. No sector can be said to be free from IRB; therefore, the security force should not lose its guards. IRB can lead to data loss

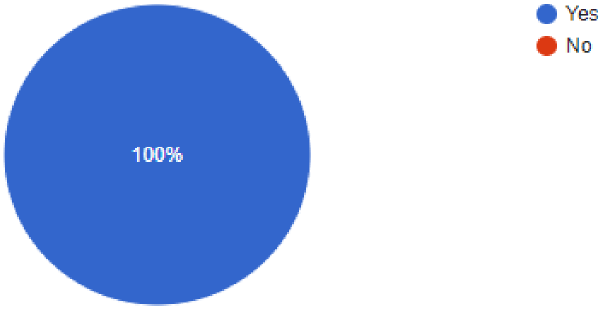

Fig 4: Data Loss Resulting from IRB

All respondents also agreed to the fact that IRB would lead to data loss. Then, organisations should endeavour to IRB at bay to prevent loss of data.

Can someone fall a victim of IRB unknowingly?

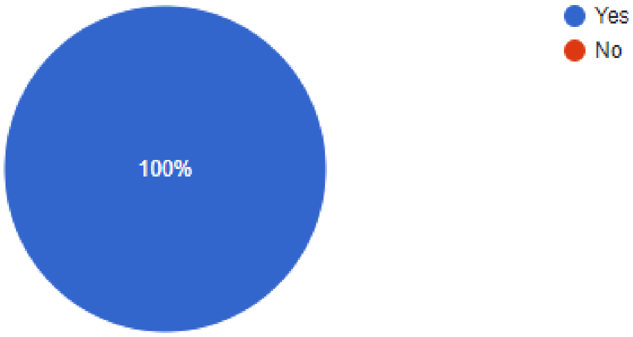

Fig 5: Inadvertent Disclosure

Fig 5 shows that one can be a victim of IRB unawares, thereby divulging sensitive details to a criminal. This may bring untold havoc upon the victim organisation.

Who is more vulnerable?

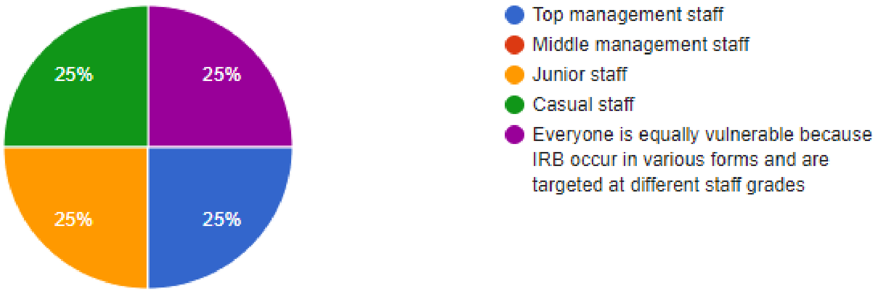

Fig 6: All Categories of staff can be Vulnerable

The survey also discovered that all categories of staff, whether low, high or middle, can be equally vulnerable – strata notwithstanding, anyone can be vulnerable.

We can protect against IRB by encryption

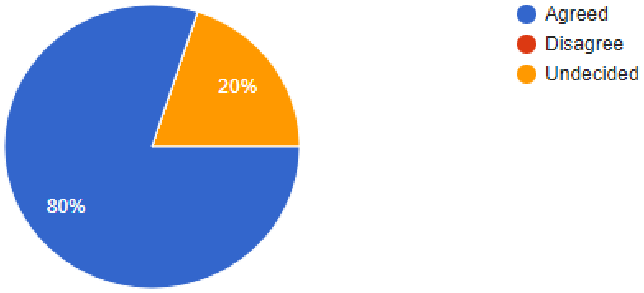

Fig 7: Protection by Encryption

While a small percentage of respondents were undecided on the issue of protection, 80% held that encryption is a good way to protect against IRB. By this, sensitive information, details or data can be shielded from attackers through cryptographic means. This study, thus, leverages encryption to protect against IRB. In particular, traditional or symmetric encryption is used.

Encryption

Encryption is a method of preserving confidentiality by converting data into that is not readily readable by a third party. Readability resides with the sender and the agreed recipient. It is a basic building block in cybersecurity as data or information flows from sender to receiver through a medium following a certain protocol. Encryption is categorised into two types: Symmetric and Asymmetric. The former is when the same encryption key is shared between the two communicating parties, while dealing with different keys between the two.

The encryption process entails making a message (called plaintext text) pass through an encryption process to be called a ciphertext text but goes through a decryption process to be converted back to a plaintext, as shown in Fig. 1.

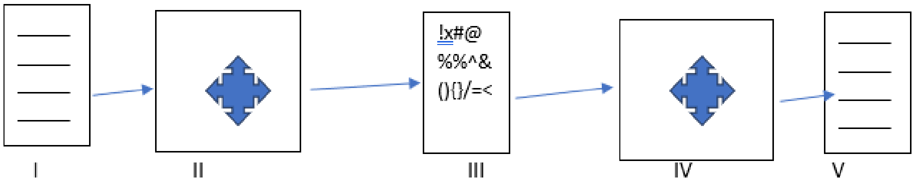

Fig: Encryption Process

Fig 1 shows the five stages of the symmetric encryption. Stage I is the plain text from the sender that is made to pass through an encryption algorithm to become unreadable by an intruder, as seen in Stage III. Before it gets to the recipient at stage V, the ciphertext in stage III is made to pass through a decryption algorithm (stage IV) so that it can be translated to something that is readily readable by the recipient who has the key. This then illustrates why an intruder would not be able to read a message as it passes through the secure channel that is encrypted. For as long as the key is unknown, it is difficult to guess what the message is. Mathematically, let there be an originating message X in an Euclidean space such as $X \epsilon X_n$ and let us assume an encryption key K defined as $[K_1, K_2, ..., K_j]$. If the encryption algorithm gives a ciphertext $Y \epsilon Y_m$. Y can then be expressed as a function of encryption E as:

$Y = E(K,X)$ ---(1)

For the Decryption with the decryption key D, then the plaintext

$X = D(K, Y)$ --(2)

An attacker observes encrypted message Y without the key K or plaintext X and wishes to recover X or K or both X and K, which becomes extremely difficult from (1) and (2).

2. RELATED WORKS

Several works have been done to secure data to prevent breaches. However, there appears to be a gap in the aspect of preventing IRB, whether at streaming, transmission, cloud computing, storage or preparation stages. A couple of works reviewed also corroborated the fact that encryption can minimise breaches. Erinle et al (2023) employed encryption to protect against vulnerabilities in cryptocurrency. In the same way, Ghiasi et al (2023) saw cryptography as a mechanism for defending against breaches in energy systems. Naheem (2023) stressed the importance of encryption in his analysis of network security. Raptis & Passarella (2023), while working on data streaming with Apache Kafka, underscored the importance of encryption. The concept of big data reminds everyone that it is ubiquitous and that security is essential to avoid breaches (Taherdoost 2023 and Yang et al, 2023).

3. CONCLUSION

Conclusively, insider-related breaches are on the increase. Being aware, from this study, that anyone can be a victim irrespective of position or sector being played can fall a victim. Loss emanating from such breaches can be much greater depending on the enormity. While a single-size-fits-all approach may be counterproductive, encryption can offer a secure means to defend against insider-related breaches.

REFERENCES

Chen, X., Hillary, G. and Tian, X. (2019). Data breach disclosure and insider trading. McDonough School of Business, University.

Erinle, Y., Kethepalli, Y., Feng, Y., & Xu, J. (2023). SoK: Design, Vulnerabilities and Defense of Cryptocurrency Wallets. arXiv preprint arXiv:2307.12874.

Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research, 215, 108975.

Health and Human Service (2022). Insider threats in health care. HHS cybersecurity program. TLP: white, ID# 202204211300

Karthiga, S., & Velmurugan, T. (2020). Enhancing Security in Cloud Computing using Playfair and Caesar Cipher in Substitution Techniques. International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN 2278-3075.

Mazzarolo, G. and Jurcut, A. (2019). Insider threats in cybersecurity: the enemy within the gates. https://www.researchgate.net/publication/337438838. DOI: 10.48550/arXiv.1911.09575. Accessed August 20, 2024

Naeem, H. (2023). Analysis of Network Security in IoT-based Cloud Computing Using Machine Learning. International Journal for Electronic Crime Investigation, 7(2).

Raptis, T. P., & Passarella, A. (2023). A Survey on Networked Data Streaming with Apache Kafka. IEEE Access.

Sharma, A., Vanjani, P., Paliwal, N., Basnayaka, C. M. W., Jayakody, D. N. K., Wang, H. C., and
Muthuchidambaranathan, P. (2020). Communication and networking technologies for UAVs: A survey. Journal of Network and Computer Applications, 168, 102739.

Schulze, H. (2024). 2023 Insider threat report. Cybersecurity Insiders. www.cybersecurity-insiders.com. Accessed August 7, 2024

Taherdoost, H. (2023). Blockchain and Machine Learning: A Critical Review on Security. Information, 14(5), 295.

Whitelaw, F, Riley, J and Elmrabit, N. (2024). A review of the insider threat, a practitioner perspective within the UK financial services, IEEE Access, vol. 12, pp. 34752-34768. https://doi.org/10.1109/ACCESS.2024.3373265

Yang, J., Chen, Y. L., Por, L. Y., & Ku, C. S. (2023). A systematic literature review of information security in chatbots. Applied Sciences, 13(11), 6355.