Integrating Cyber Forensic Analysis into Real Estate Investment: Enhancing Security and Boosting Investor Confidence

MARTINS AWOFADEJU[1], OBAH TAWO[2], BERYL FONKEM[3], CARL AMEKUDZI[4], AFOLAYAN AYOKUNLE FADEKE[5], REENA FAISAL[6]

[1] Department of Criminal Justice, College of Public Affairs, University of Baltimore, Baltimore Maryland, USA

[2] Department of Computer Science, Wrexham University, Wrexham, Wales, United Kingdom.

[3] Business Administration (Accounting), Fenimore & Fisher College of Business, Oral Roberts University, United State

[4] Department of Information and Telecommunications System, Ohio University

[5]Department of educational management, Faculty of education, University- Ekiti State University, Ado Ekiti, Nigeria

[6]Department of Finance, College of Professional Studies, Johnson and Wales University, Rhode Island, US

Abstract- The increasing cybersecurity threats to the real estate (RE) industry have to be combated using different means and strategies. This study proposes significant integration of CFA into RE as a means of enhancing security and boosting investor confidence. It relies on secondary data, drawn largely from the internet and subjected to systematic review, and employing thematic and content analyses alongside their plausible tools. Qualitative method and analytic descriptive design are employed. The analysis demonstrates that integrating CFA into RE can undoubtedly enhance security and boost investor confidence in the RE industry. The study concludes that CFA plays a significant role in enhancing security and boosting investor confidence, which lead to market stability, profit maximization, optimization, efficient service delivery and clientele safety and satisfaction. The study recommends CFA alongside other technological and conventional techniques to RE firms for quelling cybersecurity threats.

Indexed Terms- Integrating, Cyber forensic analysis, Real estate investment, Security, Investor confidence

I. INTRODUCTION

The heavy reliance of the real estate (RE) on digital operations, transactions and data management has made the industry become vulnerable to cyber attacks (Saeed et al., 2023; Mishra et al., 2022). As Mishra et al. (2022) and Bouveret (2018) show, cybersecurity attacks adversely affect all and sundry in a nation, and to avoid the escalation of the threats, strident laws and measures have to be put in place. To that end, this study proposes the integration of cyber forensics analysis (CFA) into RE. The study argues that significant deployment of CFA would enhance security in RE and boost investor confidence. Studies have explored cybersecurity threats and proffer different scholarly solutions. The present one takes up a unique dimension and a nuanced approach to the matter.

In recent times, there are increasing numbers of literatures on technology-based measures for combating cyber threats to humans, the non-humans, assets, infrastructure, finance, property, resources, and what have you (Akinola, 2024; Akinola et al., 2024;Kodete, et al., 2024; Okusi, 2024; Pasupuleti, et al., 2024; Thuraka et al., 2024; Singh, 2024; Adefemi et al., 2023; Juhrich, 2023; Bulama & Shirivastata, 2022; Li & Liu, 2021; Thakkar & Lohiya, 2021; Perwej et al., 2021; Qasim & Kharbat, 2020; Yigitcanlar et al., 2020; Al Mutawa, 2018; Shabani, 2016). Okoro and Ayaba (2023) decry the growing spates of cyber threats to RE and other sectors of society. Aikpokhio et al. (2024) and Houwayji (2024) emphasize the dire need for viable measures to be developed and sustained against cybercriminals across nations. The huge losses to cybercrimes are lamented by Aldasoro et al. (2020) and Gallaher et al. (2006), among others.

Considering the increase in the attacks, it is logical to think that the current measures for repelling the attacks are either inefficacious or less productive. To end, this study considers significant integration of CFA into the RE industry as a viable means of repelling cyber attacks, ensuring security, and transparent transactions, boosting investors' confidence, and attaining market stability in the industry. The integration requires the incorporation of the practicable tools of CFA into real estate investment and management strategies to achieve the targeted goals or results. This study considers the aforementioned as what would enhance security in the RE industry and boost the confidence of investors at a reasonable extent.

Aim and objectives

The aim of this study is to explore the role of CFA in identifying and mitigating cyber threats in RE. Its specific objectives are to:

(i) Examine the role of CFA in ensuring security and transparent transactions in RE.

(ii) Ascertain the extent to which significant integration of CFA into real estate investment can safeguard against cyber attacks.

(iii) Demonstrate that integrating CFA into RE would boost investor confidence.

Research questions

The following research questions are designed to guide the study:

(i) What is the role of CFA in ensuring RE security and transparent transactions?

(ii) To what extent can the significant integration of CFA into RE investment safeguard against cyber attacks?

(iii) Can integrating CFA into RE boost investor confidence?

State of the problem

Given that the real estate industry heavily relies on digital transactions, it is becoming increasingly vulnerable to cyber threats, which make (prospective) investors to lose confidence. Upon losing confidence, they contemplate investment into the industry. To boost their confidence, strong technology-based security measures have to be taken. To that end, this study proposes the significant integration of CFA into RE investment, as a viable means of enhancing security and boosting investor confidence. Its clarion call to action is informed by the fact that while AI in cyberscecurity obtains currently at an insignificant ratio in the RE industry, CFA is yet to be integrated into the industry accordingly.

Also, while there are increasing numbers of literatures on security threats and AI use in RE industry, none of them engages specifically with the integration of CFA into the industry to enhance as well as increase security and boost investor confidence. The foregoing points highlight the novelty of this study. Besides filling an erstwhile laid-bare research gap, it rouses deserving attention to the neglected issues of investors' loss of confidence in RE industry, as a result of the rising cyber threats to the industry.

Rising Incidents of Cyber Threats in Real Estate Industry

The 21st RE industry is characterized by pronounced digital marketing, property management, and transactions (Perwej et al., 2021; Bashroush & Schatz, 2017). Thus, there is the dire need for the deployment of robust measures that are result-oriented to tackle the cyber threats to the aforementioned aspects of the industry, with a view to restoring the confidence of investors. To achieve these goals, CFA has to be imbibed significantly and sustainably. This kind of analysis entails collecting, preserving and presenting digital evidence in legally permissible manners. CFA is a sub-field of computer science, which combines law, and investigative processes and techniques of information collation, processing, transmission, management and analysis (Homem, 2018). The goal is to analytically, empirically and evidentially unveil data breaches, fraud, and other kinds of cybercrimes.

In real estate, CFA involves collecting, investigating, analyzing and managing data breaches, and investigating property listings that may compromise critical or sensitive client information. The importance of CFA in real estate industry cannot be overemphasized. As the industry has become vulnerable to cybercriminals, cybersecurity has to be strengthened using every pragmatic measure. CFA is a technology-based means of dealing with the cyber threats confronting the industry. These criminals are deeply interested in real estate because of the huge amounts of money involved in the businesses of the industry. Since transaction details, financial records, adverts, and personal information are stored digitally, cybercriminals hack these, and pose various kinds of threats to them.

As such, they lodge different cyberattacks on the industry. These include defrauding investors, which raises contempt, fear, distrust and loss of confidence in the minds of investors, existing and prospective ones alike. Once they succeed, huge financial and data losses are recorded; the hard earned reputation of the firms involved is damaged; and legal corollaries are faced by the firms. Once they succeed, huge financial and data losses are recorded; the hard earned reputation of the firms involved is damaged; and legal corollaries are faced by the firms. Cybercriminals impersonate legitimate individuals in the industry and defraud investors. They send scam emails and even social media messages to clients.

Upon hacking accounts, personal information and financial records of real estate firms, cybercriminals post as the particular firms, send messages to redirect funds, make bargains on property branding either fake data or the original ones they had hacked from the owners, and finally defraud existing and/or prospective clients of given real estate firms. These occurrences have been at an alarming rate. The need to halt the continuity of these cyberattacks informed this study, which proposes the deployment of CFA. The study argues the significant integration of CFA into real estate fund and resource management strategies would help to repel cybercriminals' attacks, unveil and frustrate their attempts, increase security in the industry and boost the confidence of investors. If investors have (full) confidence in the industry, they would do business with real estate firms wholeheartedly. In that case, market stability obtains and the firms in the industry make profits.

Methodology

The study deploys the analytic descriptive design and the qualitative approach. It relies largely on secondary data. Additionally, observation, professional introspection and experiential learning are the primary sources relied on. The data are synthesized and analyzed thematically and content-based. Saunder et al. (2023) point out that thematic analysis paves way for an assessment of different qualitative data, drawn from different sources and themes, which are synthesized and analyzed systematically for scholarly evidence. Additionally, the secondary data in particular are subjected to a systematic review. The data include articles, theses, narrative scripts, special documents and other scholarly materials accessed from the internet.

Saunder et al. (2023) note that the data for systematic review include articles, diaries, blog posts, interview transcripts, theses, web pages, social media, audio narrations or messages, and video files. Nunn and Chang (2020) and Grant and Booth (2009) identify four stages of systematic review viz:

- Familiarising with the thematic concerns
- Identifying the thematic framework of the study
- Indexing of themes and codes
- Mapping and interpreting the collected data, relating them to research objectives and questions.

The identified stages are followed. Exclusion and inclusion criteria of the systematic review are employed to screen out some of the sourced data, while others chosen on the basis of credibility are included in the study. Among others, thematic concerns, data sources, and the extent of relevance to the sourced data relate to the present study are the core considered factors for inclusion. The search for data involved Google Scholar, Semantic Scholar, ResearchGate, Academia.edu, Microsoft Academic, CORE, and RefSeek. The overall analysis of the data is qualitative and descriptively analytic, based on the adopted design and method.

Data Presentation

Here, findings of some of the included literatures are presented for scholarly evidence. Following the synthesis of data from observation, introspection and experiential learning, the explanations given after the tables are without citations.

Table 1: Randomized findings of selected literatures

S/N	Authors & Year	Findings
1	Mishra et al. (2022)	The US had the highest banking cybersecurity regulatory policies on internet banking, while Canada had the highest policies on E-commerce and spam. While some countries have light laws against cybercriminals, others have harsh laws against them.
2	Houwayji (2024)	Diversification, hedging, and contingency planning are risk management practices that play a crucial role in organizations' and investors' financial risk management. Lebanon financial markets have been facing internal and external pressures.
3	Aikpokhio et al. (2024)	Risk identification, assessment, response planning, and monitoring and control were fund to improve cost performance. That is, these four risk variables reduce cost by 26–45%, with monitoring and control being the most influential with about 45%. Risk response planning showed 26% influence, the lowest.
4	Okoro and Ayaba (2023)	With literatures by Australian authors being the highest in number, the systematically reviewed literatures on RE investment trusts (REITs) in decision and research investments across Australia, Italy, Singapore, and Canada between 2008 and 2023 showed a significant increase. Apart from engaging with the portfolio measurement of REITs, the examined publications focused on risk assessment and management in diversified portfolios, efficiency extent, capital structure, corporate governance, portfolio creation, and strategies for asset allocation.
5	Aldasoro et al. (2020)	Larger operational losses obtain when during credit booms and excessively accommodative monetary policy. Losses to cyberattacks are small integral parts of operational losses, which can account for the total value risks of an organization.

Source: Author, 2024

By integrating CFA into RE investment and management strategies, regular audits, evaluations, and predictions are carried out by RE organizations to strengthen the security of their critical infrastructure. These enable the organizations to make informed decisions and corrective measures that prevent threat occurrences. CFA is a means of ensuring firms' compliance with legislations. Since CFA helps organizations to comply with established legal frameworks that bind on RE firm. During audits, CFA can help in providing the needed documents that prove firms' compliance with laid-down laws. This helps to build trust with clients and stakeholders. To that end, the confidence of existing and prospective clients gets strengthened. This means that CFA has the capacity of boosting the confidence of investors.

The integration of CFA rouses the confidence of investors. This is because they are sure of secured transactions and the protection of their property at a reasonable extent. Organizations that significantly integrate CFA into their RE operations prove themselves to be concerned with customer satisfaction. The satisfaction can lead to more clients, referrals, business deals, and profits. It is with commitment that organizations can meet the needs of their clients, customers, partners, investors and stakeholders. The integration of CFA into RE ought to take cognizance of the following factors:

- Evolving sustainable cybersecurity strategies that are result-oriented and problem-solving
- Put in place efficient risk management measures and modalities
- Enhance high level of awareness and technical-know-how by investing in awareness creation and campaigns, and re/training of personnel through workshops, seminars, conferences, research, symposiums, etc.
- Significant interdisciplinary collaboration and partnership, and systemic supports: These would enhance combined efforts and multiple measures, learning and mastering best practices and how to quell cyber threats, finding solutions to serious problems confronting the industry, and liaising with forensic experts, security intelligence department, the media and other agencies
- Exploit technology-based solution mechanisms, such as CFA, intrusion detection systems, secure communication platforms, encryption tools, techniques of machine learning, deep learning, computer vision techniques, and natural language processing, other AI algorithms, smart technologies, and applications
- Creating well-planned, strategically positioned, robustly designed, comprehensive, pragmatic and sustainable incident response protocols, and support systems
- Impact assessment, audits, stakeholder consultation and communication, and effective responses to and compliance with regulations.

Table 2: CFA Enhances RE Security and Investor Confidence: Scholarly Evidence

S/N	Authors & Year	Findings
1	Al Mutawa (2018)	Digital forensics models are effective tools for undertaking behavioral analysis (BA), investigation and pragmatic solutions to varied problems.
2	Ul Haque et al. (2023)	Cyber forensic investigations (CFIs) can adequately mitigate cyber threats and improve security.
3	Dwivedi et al. (2024)	Cryptographic cloud forensics technique can improve security, increase cloud-based machine learning systems, facilitate evidence-gathering investigation, secure multi-party calculation, and handle delicate information without any data breaches or harms. Decision trees (DT) and random forests (RF) detect assault accurately and undertake standard and high level of encryption of different kinds.
4	Rich and Aiken (2023)	CFA, which can enhance security against cyber attacks, also plays critical role in predictions when combined with other mechanisms like cyberpsychology.

Source: Author, 2024

Indeed, CFA can play a critical role in ensuring real estate security, investment and transparent transactions. The existence of these variables would boost investor confidence and enhance market stability. Profit maximization and progress follow suit. In the event of a cyber incident, having a cyber forensic analysis framework in place can significantly enhance an investor's ability to respond and recover. Forensic experts can quickly identify the source of a breach, assess the extent of the damage, and implement measures to mitigate further risks. This rapid response can minimize financial losses and protect the firm’s reputation.

CFA is a mechanism for prompt response to incidents and timely recoveries, since it makes it possible for investors to respond to incidents quickly. At the same time, with CFA, forensic experts are able to promptly identify sources of threats and weigh the extent of damages caused by cyberattacks. Assessment and implementation measures for effective mitigation of risks are some other benefits of CFA in real estate. Following the rapid response to incidents, losses are averted or obtained less. Losses include financial losses and damaged reputation of RE firms.

The destruction of a firm's reputation is even worse than financial loses. This is because a firm can easily get back to its fitting after some financial losses, but may not survive the aftermaths of destroyed reputation. This is why organizations do not take threats to their reputation lightly and thereby sue for damages to their hard-earned reputation. As such, to prevent threats to or destruction of reputation, CFA is imperative. Property listings, business deals, transaction details, financial records, and client data, among others, are the sets of critical or sensitive data handled by RE organizations. These require maximum protection from cyber attacks. CFA is a reliable measure for attaining the needed protection. The Table 3 below shows how cyber forensic analysis can enhance security and boost investment confidence:

Table 3: CFA benefits to RE security & investment

S/N	Variables
1	Thorough assessment and management of risks
2	Ensuring diligence in transactions
3	Prompt response to incidents and timely recoveries
4	Protection of sensitive data and critical infrastructure
5	Compliance with established legal guidelines & regulations
6	Enhancing security against cyber attacks, organizational image or reputation, building or increasing trust, and boosting investor confidence
7	Optimization, efficiency, maximal performance and results, profit maximization and market stability

Source: Authors, 2024

Following its ability to conduct thorough risk assessments, cyber forensic analysis enhances security and greater investment opportunities in real estate. As such is beneficial to integrate cyber forensic analysis into real estate investment. By analyzing past incidents of crimes in the industry, valuable factual predictions are made and recurrence averted. The proactive measures taken and put in place prevent recurrence or high rate of cyber attacks on the industry (Ahmad et al., 2020). Also, the integration of cyber forensic analysis into real estate investment can lead to reasonable extent of diligence and transparency in transactions, which undoubtedly make a splash to investors. With this technological technique in place, investors can verify the authenticity of property listings and thereby stay clear of fraudulent listings and schemes.

In other words, the integration of cyber forensic analysis into real estate investment can make it difficult fraudsters to cajole and defraud investors. This is because investors can easily verify the authenticity of any listings. The verification includes examining digital footprints for confirmation of legitimate sellers and properties. Examples of the footprints include IP addresses and transaction histories. The overall implication of the foregoing is that the significant integration of CFA into the industry can safeguard the industry against cyber attacks to a great or an appreciable extent, and boost investor confidence.

Impact

The significance of the study cannot be overemphasized. This is in view of its novelty and significant contributions to the RE industry, knowledge, research, development and combating security threats to lives and properties in estates and the RE industry. Also, the study is significant in that it concerns itself with proffering technology-based solutions to the cyber threats to the industry. The interests of the industry's investors are of prime concern to this study. By raising concerns about investors losing confidence in the business to cyber threats, the study is practically novel, innovative and impactful.

More so, by adopting a pragmatic approach to tackling cyber threats to the industry, the study is undoubtedly significant in various regards. It is of great value to RE firms, investors, fund and project managers, regulatory bodies, scholars, researchers, students and teachers. The study serves as roadmap for real estate professionals, investors and cybersecurity experts to be more proactive, predictive, decisive, security-conscious, tech-savvy, problem-solving, and protective of critical infrastructure, towards building and boosting confidence and maintaining transparency and trust. The overall impact of the study is evident in the subsequent changes, improvements, best practices, increased or maximum security against cyber attacks in the RE industry, and market stability that would aptly fall into place in the industry. These feats, which will obtain if CFA is imbibed and sustained in the industry, are symbolic impacts of this study.

CONCLUSION

For individuals, groups, organizations, industries and nations to do well and succeed maximally in the digital world, they must take cognizance of and consistently exploit technological innovations for solutions to problems so as to attain betterment, progress, success, safety and so on. This study explores the dynamics of cybersecurity threats to RE in relation to investor confidence, underscoring the crucial role of cyber forensic analysis (CFA) in ensuring security and boosting investor confidence in the RE industry. It emphasizes the need for RE firms to significantly integrate CFA into their operations to enhance security and boost their confidence of investors. It goes on to highlight the benefits of doing so and identifies factors the firms have to consider in integrating CFA into RE operations to enhance maximal or considerable security and boost investor confidence at a high extent. The study shows that ensuring security and boosting investor confidence entails a lot of multidimensional approaches and measures. The essence of this paper's clarion call for technology-based solutions to the cyber threats confronting the industry to enhance appreciable level of security and boost investor confidence. Upholding and attaining effective security measures imply showcasing organizational dedication to corporate social responsibility. The managements or managerial bodies of RE firms are majorly responsible for the task of ensuring the significant integration of CFA into RE. Thus, the leaders of RE firms ought to rise to the challenge of tackling the worrisome cyber threats confronting the industry so as to enhance security, boost investment confidence, build trust and imbibe best sustained best practices, including transparent transactions.

RECOMMENDATIONS

Beyond prioritizing security, customer satisfaction, and investor confidence, and building technology-based security culture in the industry, RE firms are charged to:

- Train and retrain their personnel on best practices and arm them with the required skills for repelling cyber security threats, which can be attained through seminars, workshops, conferences, simulations, symposiums, webinars, etc.
- Invest into efficient leadership, and strategic people and resource management, including allocating resources
- Increasingly and consistently create awareness, security initiatives, programs and measures, and work-friendly environment
- Constantly and effectively communicate with stakeholders on potential risks, strategic initiatives, performance appraisals, audits, best practices, etc.
- Cultivate, showcase and sustain transparency in operations and financial dealings with clients and investors.
- Seek attention and supports from government and its regulatory agencies for assistance
- Strong mutual and collaborative partnership with other different reputable RE and conventional organizations
- Deploying other technology-based techniques for combating cybersecurity threats, such as other blockchain, AI and smart technologies, applications and algorithms proven to be effective for security control.
- Strive to meet stakeholder needs and interests, and comply with corporate governance policies and ethical practices concerning RE.

REFERENCES

[1] Adesola Samson Adetunji ; Ayokunle Afolayan ; Toyosi Olola ; Berly Fonkem ; Rofiyat Odunayo . "An Examination of the Effects of Culturally Relevant Engineering Design on Students' Perception and Engagement in K-12 Stem Classrooms" Iconic Research And Engineering Journals Volume 7 Issue 5 2023 Page 294-300

[2] Adesola Samson Adetunji ; Ayokunle Afolayan ; Toyosi Olola ; Berly Fonkem ; Rofiyat Odunayo . "Enhancing STEM Education through Culturally Relevant Engineering Design: A Mixed-Methods Approach to Improving Student Retention and Engagement" Iconic Research And Engineering Journals Volume 7 Issue 1 2023 Page 618-627

[3] Adefemi A., Ukpoju, E. A., Adekoya, O., Abatan A., & Adegbite, A. O. (2023). Artificial intelligence in environmental health and public safety: A comprehensive review of USA strategies. *World Journal of Advanced Research and Reviews*.

[4] Ahmad, A., Desouza, K., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of security management and incident response enables organizational learning. *Journal of Association for Information Science and Technology,* 7(8), 939-953. Doi:10.1002/asi.24311

[5] Aikpokhio B. N., Gambo N., Ogedengbe F. A., & Nwoye M. I. (2024). Risk management practices and performance of construction projects: Evidence from selected estate management companies in FCT Abuja. *European Journal of Logistics, Purchasing and Supply Chain Management*, 12(1), 1-19.

[6] Akinola, A. P. (2024). Leveraging cost-effective AI and smart technologies for rapid infrastructural development in USA. *African Journal of Advances in Science and Technology Research, 15(1*), 59-71. https://doi.org/10.62154/rktd4f30

[7] Akinola, A. P., Thuraka, B., & Okpeseyi, S. B. A. (2024). Achieving housing affordability in the U.S. through sustained use of AI and robotic process automation for prefabricated modular construction. *African Journal of Advances in Science and Technology Research*, 15(1), 122-134. https://doi.org/10.62154/53t99n63

[8] Al Mutawa, N. A. (2018). Integrating behavioural analysis within the digital forensics investigation process. A thesis submitted in partial fulfillment for the requirements for the degree of Doctor of Philosophy at the University of Central Lancashire.

[9] Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks: In the financial sector. *Monetary and Economic Department, Bank for International Settlements*, no.840.

[10] Bashroush, R., & Schatz, D. (2017). Economic valuation for information security investment: A systematic literature review. *Information System Frontiers,* 19(5), 1-55. Doi:10.100/s10796-0169648-8

[11] Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. *IMF Working Paper*, 1-28, Strategy, Policy & Review Department.

[12] Bulama, L. & Shirivastata, M. (2022). The role of information & communication technology towards protection of lives and property in northern Nigeria: A focus on Maiduguri Borno State in vidyabharti.*International Interdisciplinary Research Journal*, vol.14, no.1, 1–9.

[13] Dwivedi, A., Kumar, H., Upadhyay, R. K., Chand, J., Singh, P., & Vishwakarma, R. K. (2024). A cryptographic cloud forensics method for machine learning to increase security. *Educational Administration: Theory and Practice,* 30(4), 936-942. Doi:10.53555/kuey.v30i4.1592

[14] Gallaher, M.P., Rowe, B. R., Rogozhin, A. V., & Link, A. N. (2006, July). Economic analysis of cyber security. Final technical report, Research Triangle Institute, North Carolina; Air Force Research Laboratory/IFGA, Rome NY. AFRL-IF-RS-TR-2006-227

[15] Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. Health Information & Libraries Journal 26(2), 91–108. doi:10.1111/j.1471-1842.2009.00848.x.

[16] Homem, I. (2018). Advancing automation in digital forensic investigations. Academic dissertation for the degree of doctor of philosophy in computer and systems sciences at Stockholm University. Department of Computer and Systems Sciences Stockholm University.

[17] Houwayji, S. (2024). The influence of risk management practices on financial market

stability: Insights from Lebanon. *Dutch Journal of Finance and Management*, 7(1), 25671. https://doi.org/10.55267/djfm/14181

[18] Iyanuoluwa Simon Bolarinwa ; Toyosi Olola ; Martins Awofadeju ; Beryl Fonkem . "The Death of Whistleblowing Policies in Nigeria and How It Entrenches Corruption and Financial Misappropriation" Iconic Research And Engineering Journals Volume 7 Issue 6 2023 Page 376-389

[19] Juhrich, S. S. (2023). Real-time safety technologies in the construction industry: A study of current state and challenges. Industrial design engineering, Master's Level 2023, Department of Business Administration, Technology and Social Sciences, Luleå University of Technology.

[20] Kodete, C. S., Thuraka, B., Pasupuleti, V. & Malisetty, S. (2024). Determining the efficacy of machine learning strategies in quelling cyber security threats: Evidence from selected literatures. *Asian Journal of Research in Computer Science 17 (7*), 168-77. https://doi.org/10.9734/ajrcos/2024/v17i7487

[21] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

[22] Mishra, A., Y. I.., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, 120, 102820, 1- 23. https://doi.org/10.1016/j.cose.2022.102820

[23] Nunn, J. & Chang, S. (2020). What are systematic reviews? *WikiJournal of Medicine*, 7(1):5, 1- 11. doi: 10.15347/wjm/2020.005

[24] Okoro, C., & Ayaba, M. M. (2023). Research trends and directions on real estate investment trusts' performance risks. *Sustainability,* 15, 5436. https://doi.org/10.3390/su15065436

[25] Okusi, O. (2024). Cyber security techniques for detecting and preventing cross-site scripting attacks. *World Journal of Innovation and Modern Technology*, 8(2), 71-89. DOI: 10.56201/wjimt.v8.no2.2024.pg71.89

[26] Pasupuleti, V., Thuraka, B., Kodete, C. S. & Malisetty, S. (2024). Enhancing supply chain agility and sustainability through machine learning: Optimization techniques for logistics and inventory management. *Logistics, 8, 73*. https://doi.org/10.3390/ logistics8030073

[27] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management*, 9(12), 669-710. D0I:10.18535/ijsrm/v9i12.ec04.hal-03509116

[28] Qasim, A. & Kharbat, F. F. (2020). Blockchain technology, business data analytics, and artificial intelligence: Use in the accounting profession and ideas for inclusion into the accounting curriculum. *Journal of emerging technologies in accounting*, *17(1),* 107-117.

[29] Rich, M. S., & Aiken, M. (2023). An interdisciplinary approach to enhancing cyber threat prediction utilizing forensic cyberpsychology and digital forensics. *Preprint*, 1-30. doi:10.20944/preprints202312.0770.v1

[30] Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors,* 23, 7273. https://doi.org/0.3390/s23167273

[31] Saunders, C. et al. (2023). Practical thematic analysis: a guide for multidisciplinary health services research teams engaging in qualitative analysis. *British Medical Journal*, e074256. Doi: 10.1136/bmj-2022-074256.

[32] Shabani, N. (2016). A study of cyber security in hospitality industry threats and countermeasures: Case study in Reno, Nevada. Master of science in hospitality management. University of South Florida, Sarasota- Manatee College of Hospitality and Tourism leadership.

[33] Singh, S. (2024). Benefits of an AI enabled safety management system in construction. *ResearchGate upload.*

[34] Thakkar, A. & Lohiya, R. (2021). A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research

directions. *Artificial Intell Rev.,* 55*(1),* 453–563. https://doi.org/10.1007/S10462-021- 10037-9

[35] Thuraka, B., Pasupuleti, V., Malisetty, S. & Ogirri, K. O. (2024). Leveraging artificial intelligence and strategic management for success in inter/national projects in US and beyond. *Journal of Engineering Research and Reports 26 (8*), 49-59. https://doi.org/10.9734/jerr/2024/v26i81228.

[36] Ul Haque, E., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: An analysis of the cyber threat landscape and readiness. *IEEE Access,* vol.11, 40049-40063. DOI:10.1109/ACCESS.2023.3268529

[37] Yigitcanlar, T., Desouza K. C., Butler L., & Roozkhosh F. (2020). Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. *Energies,* 13(6). Doi:10.3390/en13061473