

Comparative Analysis of Phish-Prone Rate and Asset Longevity in Information Systems

Innocent C. Atasie¹, Tin M.A Latt²

¹(IT Audits, G2GFM Management Solutions Limited, Nigeria)

²(MS Audits, GIC Myanmar, Myanmar)

Abstract:

Background: Over the last few decades, cybercriminals have deeply integrated into daily social and business infrastructure. They have devised more sophisticated means of stealing data or compromising information for financial and non-financial reasons, with attacks usually targeted at people and assets. A known social engineering technique is phishing.

Methodology: This paper examines the relationship between phish-prone rate and asset life span. A survey of 5 commercial banks was conducted for the period: Years 2023 – 2025. Questionnaires were distributed to the responsible officials from these institutions with questions relating to phishing simulation activities and asset management life cycle. Authors applied simple correlation method to validate relationship of data collected from the survey exercise.

Results: Results of the analysis showed that there is a significant relationship between phish-prone rates and asset life span. Higher prone rates lead to higher early asset retirement index (EARI).

Conclusion: This research paper has presented a comparative analysis of phish prone rate and asset longevity in information security management. Results show that user behaviour reflected by phish-prone rates can significantly impact the life span of assets.

Key Word: Phish-prone, social engineering, asset life, early asset retirement index.

Date of Submission: 29-09-2026

Date of Acceptance: 09-10-2026

I. Introduction

Growing concerns across the globe have intensified the need for improved assets and information protection. The deep and increasing desire for speed, operating costs saving, improved accessibility and systems efficiency through advancement in digital transformation has elevated the risks of cyber-attacks on assets¹. A critical concern for organisations across sectors such as banking, insurance, health care and education in this digital age, is better security for assets and systems².

Threat actors have re-engineered techniques for launching attacks to compromise data and cause disruption to business systems. These cyber criminals have consistently targeted organisations in the private and public sector with valuable and sensitive information about their staff, stakeholders, executives, suppliers and operations¹.

It is almost impossible to discuss asset and information protection without making reference to custodians, guardians, owners, and users of assets; suffice to say, human factors have direct impact on every aspect of information and asset protection. People are the most vulnerable and weakest link in protecting assets and systems. As a result of this, cyber criminals have devised more sophisticated social engineering techniques targeted at people (inside and outside the organisation)¹.

Researchers found that 95% of security incidents are caused by people – Whether intentional or not, hence technology measure is not sufficient to protect information and assets¹. Email spam filters and phishing detection methods have helped improve security and protection, although malicious emails still make their way to employee email boxes³. This implies that social engineering relies less on technological vulnerabilities but more on human psychology³.

Research by Abladi, et al⁴ argued that susceptibility to social engineering attacks has a close relationship with openness, innocence and agreeableness personality characteristics⁵. Users' ability to detect an attack could be undermined by emotional pressure, authority and greed⁶.

A good number of organisations have embraced the need to conduct regular awareness sessions for their employees, so as to explore possibilities of modifying their behavior, since many employees do not understand the implications of accessing suspicious websites, creating weak or sharing passwords, opening links in emails

from untrusted sources and disclosing of sensitive information. The need to ensure training effectiveness cannot be over emphasized.

The dissemination of phishing emails by cyber criminals has been on the increase, further sophistication of phishing techniques was mentioned by researchers¹. In this case, the receiver is presented with a link via email or other platforms (SMS, social media) and lured to click. This has resulted in severe losses and damages to assets, including reputational damage¹.

Phishing is found to be the most common method used by attackers to gain access to assets and information³. Also, phishing attacks remain popular and cost effective for cyber criminals^{7,8}. Steves et al⁹ considers access through this method as basic level access. To counter phishing activities and validate training effectiveness, organisations conduct phishing simulation to measure their phish-prone rates.

Research work by Rohani et al¹ explored cyber security scales assessing information security awareness, analysis of phishing reporting activity in a bank was discussed³, unpredictability of phishing susceptibility through experimentation was explored^{7,8,9,10,11}. Some others focused on phishing anatomy, better stimulation and mitigation measures¹². It is observed that relationship between phish prone rate and asset life management has not been considered by any published research work.

This paper explores the effect of phish-prone rates on longevity or lifespan of assets.

Research Question:

- Is there a relationship between phish-prone rate and asset lifespan?

The objective of the research is to establish a firm relationship between phish-prone rate and asset lifespan.

The paper is comprised of four parts: literature review, research methodology, Results and discussion of results, conclusion.

II. Literature Review

Social engineering is defined as a process through which cybercriminals obtain sensitive information through people, compromise systems and networks to gain access to critical data and infrastructure for financial and non-financial gains.

Common social engineering techniques – phishing, vishing, pretexting, baiting, tailgating, social media traps, were outlined and explained in great details in many research works^{4,13,14,15}. These known social engineering techniques create a sense of urgency, relies on the helpfulness or fear of the victim, exploits cognitive stress, also uses curiosity and greed, spontaneous nature of users as well as the spectacle of sheer entertainment. It could also consider appealing to user's sympathy or ego which in turn evades critical thinking⁴.

Preventive measures such as regular user awareness, phishing simulation, MFA (Multi-factor Authentication) enforcement, spam filtering, incident response planning and access control were prescribed in journals^{4,13,14}.

Rohani et al¹ paid attention to the quality of information security awareness as a way to modify employee behavior. It explored dimensions of the information security awareness and developed scales for assessing efforts and tried to educate the public regarding phishing attacks, mitigation and awareness.

Analysis of phishing reporting activity in a partner bank was presented by Doing et al³. They analysed reporting patterns as a promising indicator for the security as regards prevention of phishing.

Steves et al⁹ focused on developing a phish scale to objectively rate human detection level or difficulty. The phish scale captured number of cues, premise alignment and detection difficulty. This research was also enhanced by Sommestad et al.⁸ who suggested that a person's susceptibility depends on the phishing email, looking at three variables; Fauzan et al.⁷ provided practical guidance on protection against phishing attacks, after exploring history and evolution of phishing. Alkhalil et al.¹² evaluated and reviewed information about phishing techniques and proposed detailed anatomy of phishing to aid the development of sophisticated anti-phishing system. Knowbe⁴¹⁶ considered the implications of advancements in artificial intelligence (AI) on phishing attacks. Okokpujie et al.¹⁷ Conducted two phishing stimulations to ascertain student susceptibility in a university. None of these articles presented any relationship between phish-prone rate and asset life span, although some mentioned theft of assets as critical outcome of successful attacks. As concepts to be used in this research, it is important to understand them.

Phish-prone rate – According to Knowbe⁴¹⁶, phish-prone rate or percentage is a metric in cyber security that measures the extent or degree to which employees of an organisation are likely to interact with a simulated phishing emails, SMS or link in an unsafe way.

The phish-prone rate (%) is obtained by calculating the number of persons who click on the link divided by the number of persons who received the link. According to Doing et al.³, lower rates are seen as more secure. Phishing simulation is a technique that can be used by organisations to determine their relative phish-prone rate.

Another important concept that we will be introducing to this paper, which is synonymous with asset life expectancy is the early asset retirement index (EARI).

Early asset retirement index (EARI) is defined as the ratio of the number of assets retired before end of life to the number of assets retired at the end of life.

Recent studies have highlighted the need to further investigate the impact of phishing on systems, however the effect or relationship with asset lifespan has not explored, hence this research work.

III. Methodology

This study uses a quantitative method to assess the relationship between phish-prone rate and asset life ratio or early life retirement index.

Simple correction method will be used to compare the two variables. Data to be used for analysis will be obtained by distributing survey questionnaires to 5 commercial banks in Africa.

The correction method will enable us have an idea if there is significant relationship between the two variables under study. The degree of relationship between two variables is carried out through correlation analysis¹⁸.

The measure of correlation is called correlation coefficient (r). This correlation coefficient (r) helps to establish if there is a positive relationship (r=+1), negative relationship (r=-1) or no relationship (r=0). Pearson correlation (r) formula to be used is indicated thus¹⁸:

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

Where r = Pearson Coefficient

In this case, X will represent the phish-prone rate and Y the early asset retirement index.

Survey Questionnaires distributed to representatives of these institutions were required to provide response to the following questions; for a 3 years period (2023-2025)

1. How often do you conduct phishing simulation?
2. No of staff phishing mail was sent to
3. No of staff who clicked the link, opened or downloaded attachment?
4. Number of user end point devices
5. Number of retired/damaged end point devices
6. Number of end point devices retired before end of life.

IV. Results and Discussion of Results

Data obtained from 5 commercial banks in Africa were collated and analysed to obtain phish prone rates and early asset retirement index, X represents phish prone rates and then Y represents early asset retirement index. See tables below.

Number of email accounts that received simulated phishing mail from 2023-2025, per simulation year:

Table 1: Number of email accounts that received phishing mail from simulation exercise

12113	5025	12651	13155	13548	13669	13483
5362	13591	12475	13097	11511	10264	13781
13838	6035	13036	3950	13784	13704	13792
13887	14017	14182	4689	4504	4352	7400
3581	5698	5600	6320	3766	4319	12326
12828	13632	5960	13344	6680	7040	4135

Number of users that clicked link or downloaded attachments from 2023 – 2025, per simulation year:

Table 2: Number of persons that clicked or downloaded attachment

1533	581	606	511	1119	2100	3510
5348	1210	1202	342	641	591	795
1152	1663	133	531	60	1370	2474
4166	6314	8918	823	719	615	511
407	303	958	1004	1050	1096	1142
1188	1015	863	710	558	405	253

Number of laptops and desktops (workstations) retired within the simulation year:

Table 3: Number of retired devices

186	149	113	180	445	310
115	358	78	260	380	510

Number of laptops and desktops (workstations) retired before their end of life, within the simulation year:

Table 4: Number of retired devices before end of life

121	298	66	135	222	269
59	98	36	188	312	356

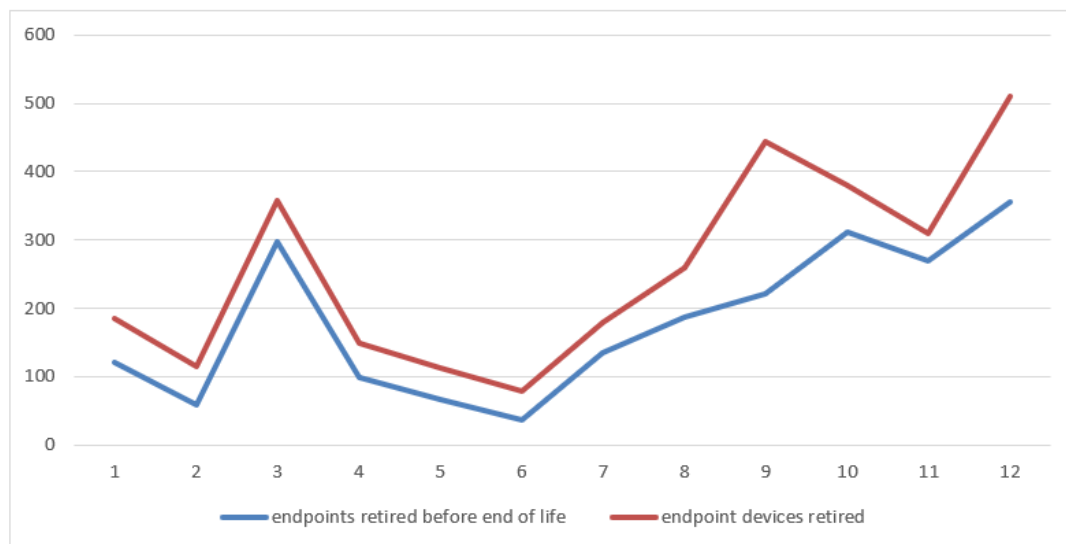


Figure 1: Line graph representation of differences in number of assets retired within simulation period.

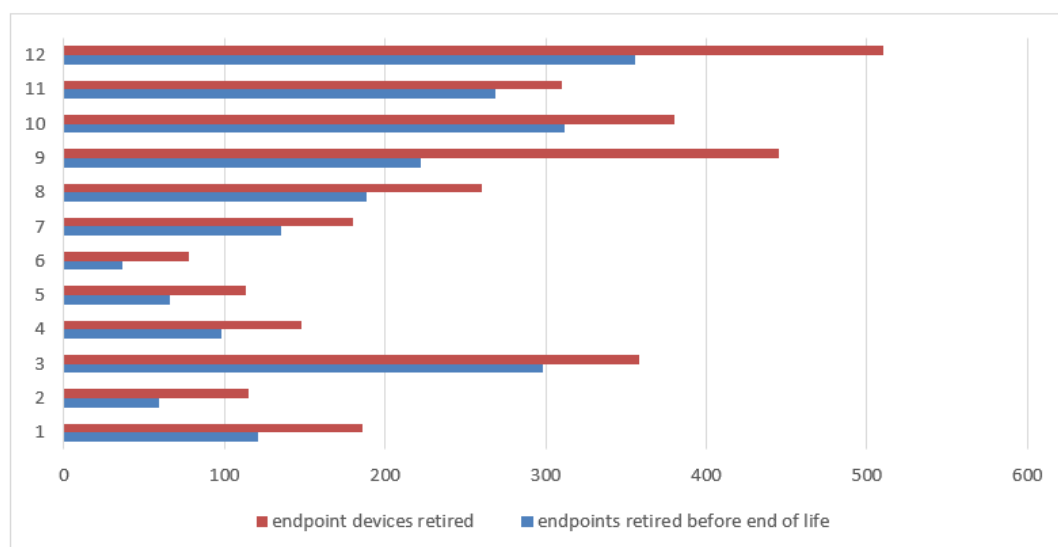


Figure 2: Bar graph representation of differences in number of assets retired within simulation period.

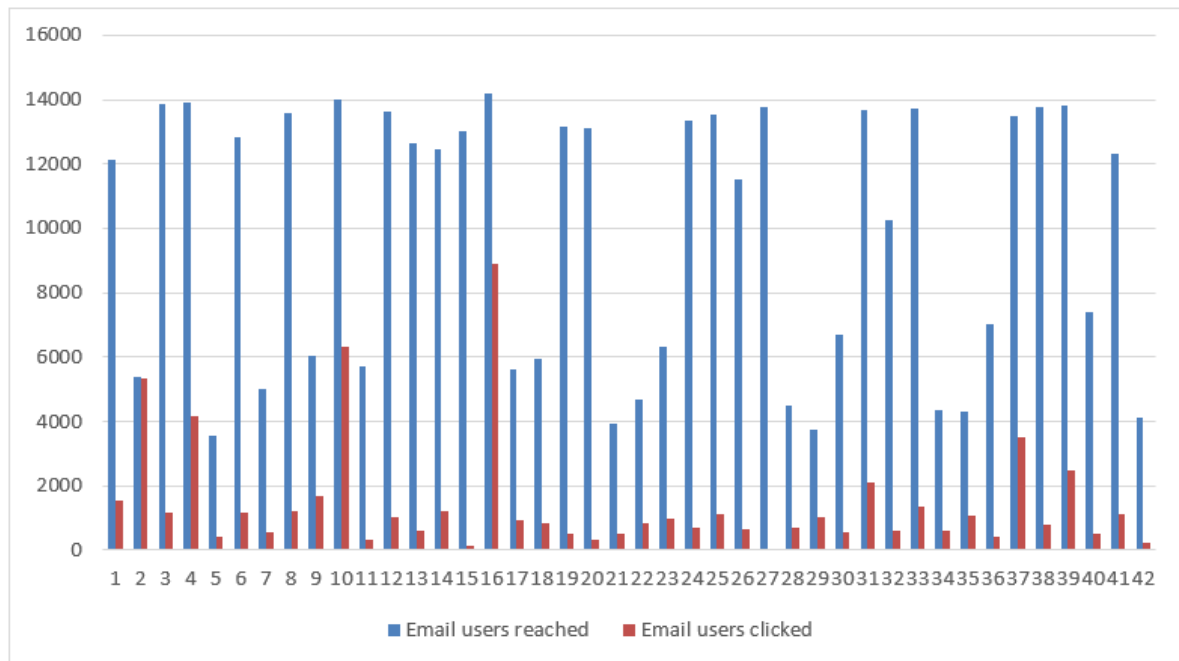


Figure 3: Cluster chart analysis of phish prone rate

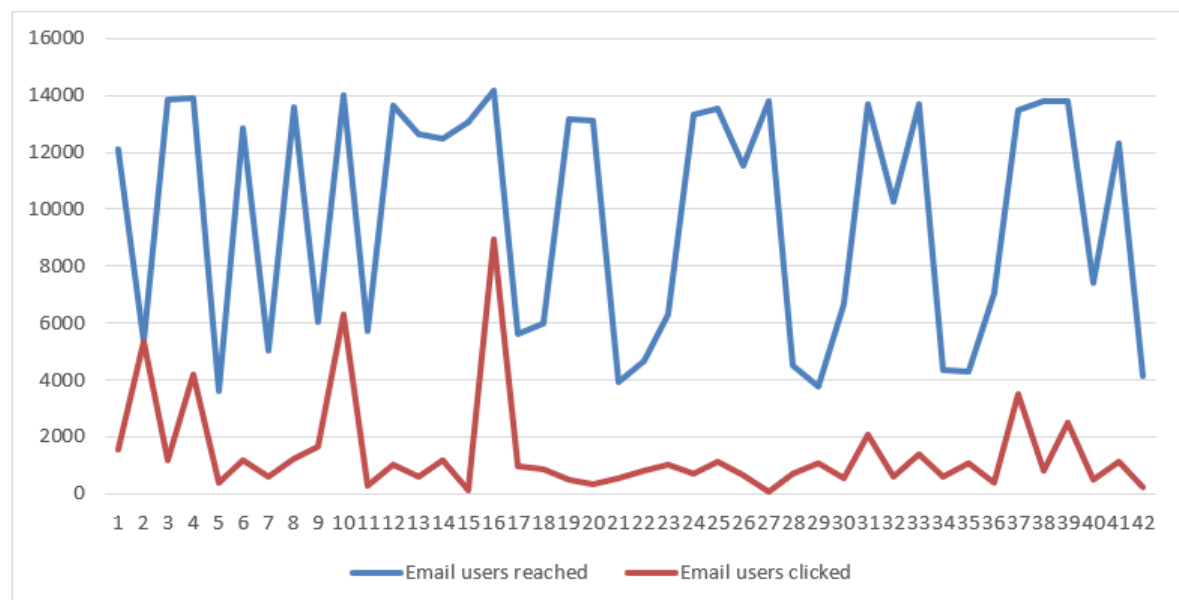


Figure 4: Line chart analysis of phish prone rate

The correlation coefficient, highlighted above was then calculated to know if there is significant relationship between phish prone rate and asset life span. The computation was done using MS Excel. The correlation coefficient obtained was $r = +0.13$, which indicated that there is some positive relationship between the variables discussed in this paper. This implies that the higher the phish-prone rate, the higher the rate of early asset retirement (or index for asset retirement).

V. Conclusion

This research paper has presented a comparative analysis of phish prone rate and asset longevity in information security management. Results show that user behaviour reflected by phish-prone rates can significantly impact the life span of assets.

References

- [1]. Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, 9(3), Article e14234.
- [2]. Biasin, E., Liguori, S., & Pato, S. (2024). Cybersecurity of AI medical devices: Risks, legislation, and challenges. In I. Glenn Cohen, T. Minssen, W. Nicholson Price II, C. Shachar, & J. V. J. M. (Eds.), *Research Handbook on Health, AI and the Law* (pp. 312–331).
- [3]. Doing, A.-K., Bárbaro, E., van der Roest, F., van Gelder, P., Zhauniarovich, Y., & Parkin, S. (2024). An analysis of phishing reporting activity in a bank. In *The 2024 European Symposium on Usable Security (EuroUSEC 2024)* (pp. 14 pages).
- [4]. Rajalim, S. (2025). Understanding human vulnerabilities: A study on social engineering techniques in cybersecurity. *International Journal for Research in Applied Science & Engineering Technology*, 13(6), 1660–1666.
- [5]. Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 8(1), 1–24.
- [6]. Alghamdi, M., & Van Moorsel, A. (2021). Decision-making under social engineering attacks: A cognitive heuristic study. In *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021)* (Article 88, pp. 1–10).
- [7]. Fauzan, P. E. P., Ubaidi, Achmad, Z., Goffäl, A., & Revi, M. I. (2024). Analysis of phishing attack trends, impacts and prevention methods: Literature study. *Brilliance: Research of Artificial Intelligence*, 4(1), 413–421.
- [8]. Sommestad, T., & Karlén, H. (2024). The unpredictability of phishing susceptibility: results from a repeated measures experiment. *Journal of Cybersecurity*, 10(1), Article tyae021.
- [9]. Steves, M. P., Greene, K. K., & Theofanos, M. F. (2020). Categorizing human phishing difficulty: A phish scale. *Journal of Cybersecurity*, 6(1), Article tyaa009.
- [10]. Karthikeyan, C., Mugilan, M., Nithish, S., Ranjithkumar, S., & Abinеш, M. (2025). Phishing attack stimulation and prevention mechanism. *International Research Journal on Advanced Engineering and Management*, 3(4), 1029–1034.
- [11]. Adewumi, S. E., & Ani, U. D. (2025). Impact of detection accuracy rates on phishing email spikes: Towards more effective mitigation. *Information Security Journal: A Global Perspective*, 34(4), 354–391.
- [12]. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, Article
- [13]. Panda, S. P. (2025). The evolution and defense against social engineering and phishing attacks. *International Journal of Science and Research*, 14(5), 1435–1440.
- [14]. Chapagain, D., Zhao, Y., Acharya, S., & Shrestha, R. (2024). SEAtch: Deception techniques in social engineering attacks: An analysis of emerging trends and countermeasures. *arXiv preprint arXiv:2408.02092*.
- [15]. Nismy, S. A. H. H., & Kajave, A. M. (2022). *How cyber criminal use social engineering to target organizations*. arXiv.
- [16]. KnowBe4. (2025). *2025 phishing by industry benchmarking report*. <https://www.knowbe4.com/resources/reports/2025-phishing-by-industry-benchmarking-report>
- [17]. Okokpujie, K., Kennedy, G. C., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity awareness: Investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (A case study of a Nigerian leading university). *International Journal of Intelligent Systems and Applications in Engineering*, 11(3s), 332–341.
- [18]. Moore, D. S., McCabe, G. P., and Craig, B. A. (2021), *Introduction to the practice of statistics* (10th ed.). W. H. Freeman.

About the authors

Innocent Chibueze Atasie is an IT Audit and Assurance Leader who has provided services across countries in Africa, Middle East, USA and Africa. He holds C|CISO, CISA, CRISC, CDPSE, CISM, CDPO certifications, 15 ISO certifications, a fellow of over 4 reputable institutions. He is the Chief Executive of G2GFM Management Solutions Limited. He holds BEng and MSc Degrees from University of Nigeria and University of Lagos. Research interests are in the areas of Information Security, IT, privacy and cloud security. He is the winner of Ron Islami Award for the MSECBA Auditor of the Year 2025 for Africa.

Dr. Tin Latt is an IRCA-registered Lead Auditor in quality management and information security management (QMS & ISMS) systems. He served on ISACA's IT Audit and Assurance Group, where he oversaw updates to the IT Audit Framework (ITAF) during the 2025-2026 terms. He currently serves as a membership assessor with AICPA-CIMA. He is professionally qualified in IT/IS auditing and holds CISSP (ISC2), AAIA, CISA, CISM, CGEIT (ISACA), PCIP (PCI-SSC), ISRM (ISCA, Singapore), CIA (IIA, USA), and ISO/IEC 27001 (BSI, UK). He has worked as an independent lead assessor for QHSE management systems, including ISO 9001, ISO 14001, ISO 45001, and ISO/IEC 27001 Information Security Management Systems. He conducted numerous training sessions in Governance, Risk, Audit, and Controls; IT Audit and Risk Management; and information and cybersecurity. He graduated with a Doctorate in Business Administration, specializing in Information Systems and Projects, from Liberty University (Virginia, USA), and an MBA from Oxford Brookes University (UK). He holds professional accountancy qualifications: FCCA, FCMA, CGMA, and CA Singapore.