Journal of Enterprise Information Management

The moderating impact of technology on cyberfraud perpetration and organisation cybersecurity outcomes

Oluwatoyin Esther Akinbowale, Mulatu Fekadu Zerihun and Polly Mashigo

Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa

Received 5 January 2026
Revised 1 April 2026
1 May 2026
18 May 2026
20 June 2026
Accepted 20 June 2026

Abstract

Purpose – This study assesses the moderating impact of technology in the relationship between cyberfraud perpetration and organisation cybersecurity outcomes such as blocked attacks, response to cyber threats, increase in uptime, reduction in financial loss due to cyberfraud, data breaches and operational disruption.

Design/methodology/approach – The study uses a quantitative survey using a questionnaire as the survey instrument to obtain a primary dataset from the 17 licensed banks in South Africa. It draws insights from the criminological and information systems theories to determine the moderating role of technology in the relationship between cyberfraud occurrence and cybersecurity outcomes. Primary data were collected and moderation analysis was carried out in the Statistical Package for Social Sciences (SPSS, version 29 environment).

Findings – The outcome of the interaction term between cyberfraud perpetration and organisation's technological ability is statistically significant and negative ($\beta = -1.462$, $p < 0.05$). This shows that technology moderates the relationship between cyberfraud perpetration and organisation's security outcomes. The results show that banks experiencing a high rate of cyberfraud perpetration are also the ones investing more in cybersecurity measures and reporting more controls and vice versa. While the preventive and especially the detective technologies significantly moderate and mitigate cyberfraud perpetration effect, the response technologies exhibit no significant buffering role, thus indicating limited effectiveness.

Research limitations/implications – The article contributes to knowledge by establishing the dual role of technology as a cyberfraud enabler and mitigator, thus advocating for its moderating role. The outcome of this study as well as the policy recommendations can assist policymakers and financial institutions in moderating technology to mitigate cyberfraud perpetration.

Practical implications – The findings and policy recommendations can assist policymakers and the banking institutions in moderating technology to mitigate cyberfraud perpetration.

Originality/value – The study is novel in that it contributes conceptually, methodologically and empirically to technology as a moderating variable between cyberfraud perpetration and organisation's security outcomes.

Keywords Cyberfraud, Cybersecurity, Banking institutions, Information systems, Moderation analysis, Technology

Paper type Research article

1. Introduction

Cyberfraud is a universal threat that affects individuals, organisations, stakeholders, public and governments. This fraud is escalating with the increasing adoption of digital technologies for financial products and services. Nonetheless, technology also plays an important role in mitigating its effect. The increase in the adoption of digital technologies for financial products and services has promoted financial inclusion through ease of access to financial service. It has also contributed positively to economic and social activities globally by enabling easy, time and cost-effective transactions. Many of the financial products and services are digital in

Journal of Enterprise Information Management
Emerald Publishing Limited
e-ISSN: 1758-7409
p-ISSN: 1741-0398
DOI 10.1108/JEIM-01-2026-0014

nature and can be accessed remotely, thereby enabling non-contact or remote operations. However, this transformation has paved the way for cyberfraud perpetration as threat actors leverage social engineering schemes such as phishing, hacking, identity theft, ransomware, etc. to commit financial fraud. Reports globally as consistently reported an increase in the frequency and impact of cyberfraud perpetration, thereby posing a significant threat to individuals, organisations, stakeholders, public and governments (Anderson *et al*., 2019).

Technology plays a dual role in this context. On one hand, the use of emerging technologies enables the threat actors to intrude into individual's and organisation's information to commit fraud, especially when the cybersecurity architecture is compromised. On the other hand, digital technologies such as data mining also serve as important techniques for threat management (Ali *et al*., 2019; Yar, 2013; Von Solms and Van Niekerk, 2013; Gordon and Loeb, 2002). Threat management encompasses the process of identifying, preventing, and responding to cyber threats in real time. Despite these dual roles played by technology (in cyberfraud perpetration and mitigation), many studies focused mainly on the causes and impact of cyberfraud perpetration and the development of cybersecurity solutions (Akujobi *et al*., 2026; Adewopo *et al*., 2025; Bukhari *et al*., 2024; Akinbowale *et al*., 2024 and 2023). Limited studies reported on the moderating role of technology in the relationship between cyberfraud perpetration and organisation's security outcomes. To address this gap, this study investigates the moderating impact of technology in the relationship between cyberfraud perpetration and organisation cybersecurity. It employs a quantitative survey using questionnaire as the survey instrument to obtain the primary dataset.

Hence, the research questions underlying this study are as follows:

(1) How does technology moderate the relationship between cyberfraud perpetration and organisation cybersecurity outcomes?

(2) What is the moderating impact of technology on cyberfraud perpetration and organisation cybersecurity outcomes?

To answer these research questions, one alternative hypothesis was formulated in this study as follows:

> Preventive, detective, and response technologies significantly weaken the negative relationship between cyberfraud perpetration and cybersecurity outcomes

This study is justified by the need to explore the interplay of technology with cyberfraud perpetration and cybersecurity. The understanding of the moderating role of technology will provide a more nuanced explanation of cyberfraud perpetration and cybersecurity. This may influence risk perceptions and management, skill requirements, detection and prevention capabilities, as well as offender's behaviour. Furthermore, technological evolution and its adoption in financial products and services have created a gap between cyberfraud perpetration and existing fraud theories such as criminology and information system theories. This study addresses this gap by highlighting technology as a major factor influencing cyberfraud perpetration and at the same time its mitigation. It contributes to knowledge methodologically and empirically by establishing the moderating role of technology in the relationship between cyberfraud perpetration and organisation cybersecurity outcomes.

The increasing rate of cyberfraud perpetration and the vulnerability of the cybersecurity system motivates the need for this study. Cyberfraud continues to pose a significant threat to individuals, stakeholders and financial institutions, causing financial losses and undermining public trust and cybersecurity systems. Threat actors leverage the ease of access and user-friendliness of emerging technologies in cyberspace to exploit the vulnerability of digital systems to perpetrate fraud. Banks and other financial institutions and risk managers may struggle to keep pace with the dynamics of the threat actors and technological evolution, leading to a reactive approach to cyberattack rather than a proactive or preventive approach.

Thus, by examining the moderation role of technology in cyberfraud perpetration and cybersecurity outcomes, this study provides insights that can support more support proactive, technology-driven solutions. Theoretically, the limited integration of technological factor into the traditional crime theories as a moderator limits their application in the digital context especially in this era of technological advancement and digitalisation.

The study is novel in that it contributes conceptually, methodologically and empirically to technology as a moderating variable between cyberfraud perpetration and organisation's security outcomes. Previous studies consider technology as a direct predictor but this this study models it as a conditional mechanism that determines the strength and direction of cyberfraud perpetration.

For instance, this study disaggregated technology into three (1) preventive technologies which reduce exposure of the victims and opportunity of the threat actors before cyberfraud occurs) in line with the routine activity theory (RAT) (guardianship). (2) Detective technologies which increase the perceived detection risk during fraud perpetration in line with the rational choice theory (RCT) (punishment to serve as deterrent). (3) Response technologies which minimises damage after cyberfraud perpetration (post-event resilience).

Thus, this study demonstrate that cybersecurity technologies can operate via three unique approaches (prevention, detection and response), each exerting different moderating effects on the cyberfraud–cybersecurity outcome relationship.

By drawing insights from the survey outcomes and theoretical frameworks such as the criminological and information systems theories, this study provides policy recommendations that can assist the banking institution to understand when and how technology exchanges its role in mitigating or exacerbating cyberfraud perpetration.

It is significant and time-driven in that it assists the banking institutions and cybersecurity stakeholders in understanding how specific technologies influence the dynamics or behaviours of the threat actors. It can also assist policy makers in the development of cyberfraud policies that will mitigate the misuse of technological capabilities or in the formulation of technology-responsive cybercrime laws. This study advocates for the responsible deployment of technologies balancing technological balances innovation with cybersecurity. Thus, the empirical findings can contribute to improved public awareness of technological risks and responsible technology use. In addition, the policy recommendations can strengthen digital trust and contribute to a safer online environment for individuals and the banking institution.

Saidi *et al*. (2024) found that cybercrime poses a significant threat to the economic security of Kenya. Their findings indicate that there is increasing Internet penetration in Africa, leading to the rapid digitalisation of the African economy. Thus, there is a need for the development of effective risk mitigation strategies.

Some authors argue that the deployment of technology in financial institutions increases cyberfraud opportunities through ease of accessibility of Internet-based systems and the creation of new vulnerabilities and adversarial risks, expansion of attack surfaces and automation of attacks (Ali *et al*., 2019, 2025; Akujobi *et al*., 2026). Other authors argue that technology is protective and can strengthen internal controls, thus improving fraud detection. Thus, there exists a consensus that technology can improve fraud mitigation but also enable sophisticated attacks depending on how it is deployed, the level of deployment, user competence and human–technology interaction, institutional and regulatory strength as well as alignment with social and technical systems (Buczak and Guven, 2016; Firdaus *et al*., 2022; Akinbowale *et al*., 2025b). This implies that technology alone cannot determine cyberfraud outcomes, as other factors such as governance, regulation, human and institutional capacity, and behavioural patterns of threat actors also play decisive roles.

2. Literature review

Studies on cyberfraud have predominantly focused on the frequency, impact, root causes and the behaviour of the threat actors. The outcome of these studies indicated an increasing trend in

the rate of data and cybersecurity breaches and cyberfraud perpetration globally with increasing dynamics in the behaviours of the threat actors (Romanosky *et al*., 2019). There is also a rising trend in the cost implications of cyberfraud coupled with loss of organisation's reputational and goodwill (Anderson *et al*., 2019). Chen *et al*. (2023) reported an inverse relationship between cybersecurity breaches and market reaction. Studies indicated that organisations with poor internal control and ineffective cybersecurity framework are more prone to cyberattacks and are more likely to suffer significant losses (Gordon *et al*., 2021; Chen *et al*., 2023).

Zulu and Boshoff (2025) stated that cybercrime effect on South African organisations can be categorised into two: the explicit effect comprising financial loss, data loss, operational downtime and the implicit effect comprising reputational damage and remediation-associated costs. The authors suggested the need for an effective response to cyberthreats via a coordinated multi-stakeholder collaboration between organisations and law enforcement agencies.

Aphane (2023) explores the level of cybersecurity awareness among youth in the Gauteng Province of South Africa. The author found that cybercrime awareness and education programmes are insufficient in South Africa. This study revealed a significant gap in public and institutional cybersecurity education, suggesting the need for the integration of cybersecurity awareness and protective behaviours into policing and community sensitisation programmes.

Adewopo *et al*. (2025) offer a regional perspective on cybercrime and its related policy issues in West Africa. According to the authors, there exist legal provisions in tackling cybercrime, but this is undermined by ineffective regional coordination and institutional lapses. The authors further suggested the need to strengthen policies aimed at cybercrime mitigation in West Africa.

Studies show that many African countries are gradually developing institutional capacities and policy responses to combat cybercrime threats; however, with varying levels of success. Kritzinger and von Solms (2012) identified four important cyber safety issues in Africa. These include policy formulation, implementation procedure, awareness level, research and the establishment of technical security processes. The authors suggested a synergised approach consisting of an integrated effort of all relevant stakeholders to cybercrime mitigation. Similarly, Snail ka Mtuze and Musoni (2023) reviewed South Africa's cybercrime law, citing inadequate enforcement and technological misalignment. This outcome agrees with the findings of Akinbowale *et al*. (2025a) that South Africa is making significant progress in the area of cybersecurity laws and policy; however, the implementation of these laws has relatively stalled the progress.

The outcome of the literature review is summarised according to the various themes in Table 1.

2.1 Interplay of technology, cyberfraud and cybersecurity

Cyberfraud is evolving rapidly together with the developments and evolution in digital technologies such as end-to-end-encryption etc.

In this era of digital banking, the understanding of cyberfraud necessitates its disaggregation into two, namely operational typologies and attack pathways (Levi and Smith, 2021; Button and Cross, 2017).

The major forms of cyberfraud include: (1) Social engineering. This involves the manipulation of people to obtain sensitive information that will be used for cyberfraud perpetration. It exploits human vulnerabilities rather than technical flaws. This could be in the form of phishing, spamming, etc. Studies indicate that social engineering such as phishing is one of the most prevalent forms (Hadnagy, 2018; Verizon, 2023). (2) Account Takeover (ATO) and Identity Theft:

The attackers gain illegal access to the victim's accounts using stolen credentials (ENISA, 2022). (3) Malware and Ransomware Attacks: This is a form of cyberfraud attack in which

Table 1. Outcome of the literature review on cyberfraud perpetration

Theme	Findings	Reference
Increase in digitalisation and vulnerability of cybersecurity infrastructure	There is a direct relationship between Internet penetration leading to growth of digital services and exposure to cybercrime risks	Akinbowale *et al*. (2025b)
Legal frameworks, policy and enforcement capacity	African legal frameworks lack enforcement capacity as a result of limited resources, insufficient training, and technological capabilities	Snail ka Mtuze and Musoni (2023), Adewopo *et al*. (2025), Akinbowale *et al*. (2025a)
Economic and social impact	Cybercrime results in economic and financial losses, and undermines public trust	Zulu and Boshoff (2025), Akinbowale *et al*. (2023)
Awareness and capacity building	There is a gap in cybercrime awareness hence the need for increased awareness, cybersecurity literacy, capacity development and educational programme to strengthen cybersecurity and to foster understanding among the stakeholders	Aphane (2023)
Collaboration	Tackling cybercrime necessitates effective collaboration between public and private sectors, and the stakeholders	Zulu and Boshoff (2025)

viruses such as Trojans and ransomware target are injected online, targeting the computer systems to either siphon funds or extort institutions. This form of cyberfraud is increasingly automated and scalable, utilising botnets and AI-enabled tools (Kharraz *et al*., 2019). (4) Insider-Enabled Fraud: Sometimes organisation's employees take undue advantage of access to customer's confidential information to override controls or commit online fraud (Greitzer and Frincke, 2010). (5) Payment and Transaction Fraud: This could take the form of unauthorised transfers, card fraud and SWIFT-related attacks perpetrated by exploiting the vulnerability of the transactional system and weak monitoring systems (SWIFT, 2020).

Beyond typologies, cyberfraud could take place through any of the following mechanisms: (1) Human Factors: This involves social engineering attacks that exploit human vulnerabilities (Verizon, 2023). (2) Technological Exploitation: This encompasses attacks that exploit the loopholes in software, networks, and authentication systems, such as malware (ENISA, 2022). (3) Process and Control Weaknesses: This exploits the loopholes in the organisation's internal controls, such as delayed system updates, and lack of real-time monitoring, etc. to perpetrate fraud (Button and Cross, 2017).

Previous research has sufficiently highlighted the causative factors such as individual, organisation's social and economic factors influencing cyberfraud perpetration (Akinbowale *et al*., 2023 and 2024), however, less attention has been given to the interplay of technology, cyberfraud and cybersecurity. Many studies have considered technology as either an enabler of cybersecurity or a mitigating factor in cyberfraud rather than considering it as a moderating factor.

The role of technology in cybersecurity cannot be overemphasised. For instance, emerging technologies such as artificial intelligence (AI) based can aid pattern recognition, threat detection, cyberattack prevention fraud classification. It could also enable real-time and automated incident response to reduce detection time and to avert severity in cyberfraud perpetration (Buczak and Guven, 2016). Some studies argue that the deployment of emerging technologies without the supporting infrastructure, required organisation's processes and enabling skills is counterproductive (Gordon *et al*., 2021). Hence, literature supports the fact that technology interacts with other factors such as human behaviour, and organisational

internal control mechanism, data, other digital technologies, etc. rather than acting independently (Akinbowale *et al*., 2024, 2025b).

While the deployment of technology is a viable and sustainable approach to cyberfraud mitigation, studies have shown that the adoption of emerging technology alone cannot guarantee cybersecurity. Cybersecurity comprises an integrated architecture comprising various elements such as system's configuration, periodic upgrade of software, end-to-end encryption, data handling, risk management, etc. and any loophole in any of the elements could undermine the technological element and, by extension, the entire cybersecurity framework, resulting in cyber-attack. This indicates that the impact of technology's on cyberfraud perpetration is contingent rather than deterministic. For instance, Anderson *et al*. (2019) indicated that digital trading such as cryptocurrencies had led to the emergence of new cybercrimes and the deployment of cloud computing technology had led to system's misconfiguration leading to security breaches, social engineering, denial of service and cybercrime perpetration. Cybercrimes keep evolving with different variants and supporting infrastructure such as botnets.

Maluleke (2023) conducted a systematic analysis of cybercrime as an increasing and intricate phenomenon in Africa. The study found that technological penetration and limited institutional capacity contributed to the surging wave of cybercrime perpetration in Africa, while noting inadequate policing and legal frameworks to address this surge. This study indicated the need for a context-specific technological approach to mitigating cyber threats within the African socio-legal contexts.

Akinbowale *et al*. (2023) and Nwafor (2024) emphasise the need for digital forensic technology for effective cybercrime mitigation due to the rising trends in cyberfraud perpetration. These studies indicated that investigative lapses frameworks weaken the successful implementation of cyber laws and the prosecution of the threat actors, suggesting the need for digital forensics and trained personnel within the law enforcement agencies. Similarly, Setona (2024) identified the roles of forensic experts in cybercrime investigations in the South African Police Service (SAPS). The authors reported that the complex nature of digital evidence warrants the deployment of forensic technology for digital evidence analysis as well as the need for forensic experts to ensure that evidence is processed in a way that it is admissible for prosecution. This reflects the need for a strong institutional capacity in the area of forensic technology deployment and human capacity development. Matsaung (2023) suggested the deployment of intelligence-based policing in cybercrime mitigation in South Africa. The authors suggested the need for synergy amongst the security stakeholders sharing and effective integration of intelligence integration as a critical component of cybercrime policing.

The outcome of the literature reviewed in this section revealed that over-reliance on technology, investigative lapses, absence of strong institutional capacity and lack of synergy among security stakeholders contribute to both cyberfraud perpetration and cybersecurity breaches. Conversely, it also highlights the capability of technology with consideration for organisation's and human factors as a mitigation tool against cyberfraud perpetration and cybersecurity breaches.

2.2 Related works

Akinbowale *et al*. (2025b) found that technology can mediate between the causes and rate of cyberfraud perpetration in South African banks. The authors found that technology can influence internal controls, accountability and ethical systems, thus reducing cyberfraud when aligned with governance structures, although it may not singularly mitigate organisational weaknesses and cyberfraud perpetration. Bukhari *et al*. (2024) focused on the relationship between AI, cybercrime incidents and organisational performance using the partial least squares structural equation modelling. The outcome indicates that the adoption of AI can moderate the impact of cyber threats on organisational outcomes. Technology can also

introduce new vulnerabilities, thus moderating the role indecisive. Thus, technology can be protective and at the same time risk-enhancing.

Olanrewaju and Adebiyi (2024) found that expansion in the mobile information communication technology increases the rate of cybercrime perpetration as a result of increase in accessibility and misuse. This implies technology can increase the capability of the threat actors and target exposure. This further suggests that technology can moderate the relationship between opportunity and cybercrime occurrence.

Widiasari and Thalib (2022) indicate that the evolution of information technology led to an increase in cyberfraud perpetration in Indonesia. This implies that technological advancements may increase cyberfraud perpetration unless an effective control mechanism is deployed.

Mushtaq and Shah (2024) indicate that technology alone cannot sufficiently mitigate cybercrime but may become highly effective when integrated with organisation's and human factors. Mushtaq and Shah (2025) further found that by integrating technology with organisation's and human factors, the rate of cybercrime perpetration may be reduced via effective system design, governance and user behaviour. Thus, the moderating effect of technology depends on the context and socio-technical factors.

Table 2 summarises the empirical literature review on how technology can serve as a mediator or moderating variable and how it influences the relationship between cybersecurity occurrence and related causes of cyber breaches.

2.3 Theoretical frameworks

This study is rooted in the criminological and information systems theories to determine the moderating role of technology in the relationship between cyberfraud occurrence and cybersecurity outcomes. Criminological theories such as the RAT, RCT and socio technical theory (STT) were considered, with technology conceptualised as a moderating variable that influences opportunity, decision-making processes and learning mechanisms in cyberfraud perpetration.

The RAT argues that crime can happen when a motivated offender meets opportunity in the absence of a capable guardian (Cohen and Felson, 1979). In cyber contexts, technology can act as a capable guardian with the capacity to provide surveillance, detection and deterrence. Conversely, technology can also promote vulnerabilities, thus increasing the suitability of the target. The RCT argues that crime can be reduced when the perceived costs of perpetration outweigh the perceived rewards or benefits. Technology can provide advanced monitoring and detection and provide evidence for prosecution, thus increasing the perceived risk for the threat actors. Hence, technology can act as a deterrent moderating cybercrime behaviour of the threat actors (D'Arcy and Herath, 2011).

STT argues that crime perpetration can be influenced by the interaction between technical systems and social structures. Here, technology moderates cyberfraud outcomes when aligned with human skills, organisational culture and governance frameworks (Trist and Bamforth, 1951).

In addition, the information systems theory, such as the technology adoption model (TAM), which argues that technological adoption is a function of the perceived usefulness and user's friendliness (Davis, 1989) was also employed in this study as part of the theoretical framework. This theory implies that an organisation's technological capability level can influence how cyberthreats translate into cybersecurity outcomes.

Figure 1 presents the overview of the theoretical framework employed in this study. The RAT provides insights into how technology moderates target suitability and guardianship, while the RCT reveals how technology moderates the perceived risk–benefit decision of the threat actors (cost-benefit calculation). The SLT provides insights into how technology moderates exposure to criminal peers and techniques as well as how technology reshapes constraints, while the TAM reveals how technology moderates the relationship between

Table 2. Outcome of the literature review on technology as a mediating or moderating variable and the cybersecurity outcomes

Reference	Focus	Moderating/Mediator variable	Outcome variable	Methodology	Key findings
Akinbowale *et al*. (2025a, b)	Causes of cyberfraud perpetration in banks	Emerging technologies serve as the mediator variable	Rate of cyberfraud perpetration	Survey and mediation analysis	Emerging technologies mediate the relationship between causes of cyberfraud and rate of perpetration
D'Arcy *et al*. (2009)	Misuse of information security in organisations	Monitoring technologies	Information security compliance	Survey and structural equation modelling	The deployment of monitoring technologies reinforces compliance and minimises the impacts of information security misuse
Ransbotham and Mitra (2013)	Security breaches in firms	Security technologies such intrusion detection system (IDS)	The effectiveness of security breach mitigation	Event study	The use of advanced technologies such as IDS reduces the severity of security breach severity and improves recovery time
Kwon and Johnson (2014)	Cybercrime incidents in firms	Information technology (IT) security capabilities	Information asset protection	Survey and regression analysis	IT security capabilities reduces the negative effects of incidents on asset protection
Ransbotham and Mitra (2013)	Cyberattacks in organisations	Disclosure	Attack diffusion and penetration of attack	Panel data	Instant disclosure of threats lessens delay in the attack diffusion process and fairly increase attack penetration but fairly decreases the overall volume of attacks
Li *et al*. (2022)	Investigation of the antecedents and mediators of employees' cybersecurity motivational behaviour	Antecedents (information security effort, employee security awareness), cybersecurity	Employees' cybersecurity motivational behaviour	Empirical data from survey and structural equation modelling	The antecedent factors correlate significantly with the cybersecurity threat and coping strategies of the threat actors, while the mediating factors were useful in predicting cybersecurity motivational activities

criminal intention and cyberfraud perpetration. It explains why offenders adopt certain tools. For instance, when the enabling technologies employed for financial services are highly user-friendly with ease of access (less rigorous authentication mechanisms), more people, including individuals with low technical skills, are more likely to engage in cybercrime. However, when the use of the technologies and access are complex, only highly skilled threat actors may proceed. On the other hand, the more complex the technology, the lower the adoption and use, especially across individuals with low computer literacy.

This study advances existing knowledge by filling the empirical gap of limited quantitative evidence examining moderation effects between cyberfraud and cybersecurity outcomes in the South African banking industry. It also addresses the contextual gaps that exist as a result of limited

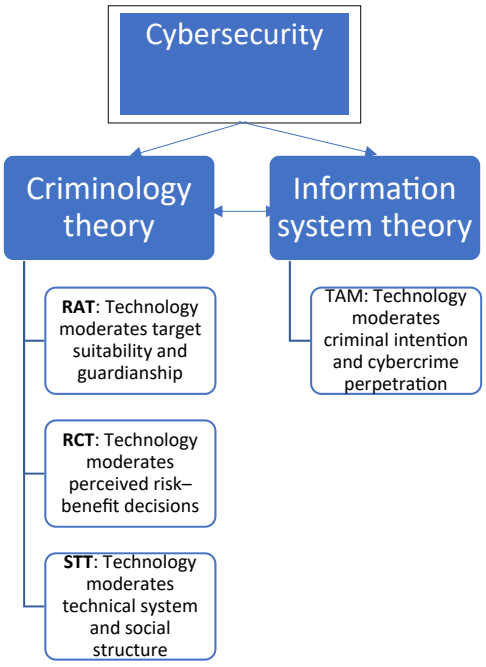

Figure 1. The theoretical framework employed in this study. Source: Authors' own work

research focusing specifically on the banking sector in developing or emerging economies such as South Africa. It addresses the temporal gaps resulting from rapid technological changes and evolving cyberfraud patterns that require updated empirical investigation.

3. Methodology

In this study, the independent variable is the cyberfraud perpetration (measured in terms of rate, scale and sophistication), while the dependent variable is the organisational cybersecurity outcomes (such as Blocked attacks, system's uptime/resilience, confidentiality and integrity). The moderating variable is technology encompassing the intrusion detection and prevention as well as authentication mechanisms).

The major proposition is that the effect of cyberfraud perpetration on organisational cybersecurity outcomes is dependent upon the level and effectiveness of technological capabilities.

The moderating role of technology is rooted in an integrated theoretical framework comprising four theories. The RAT posits that cyberfraud could be perpetrated when there are motivated offenders and opportunity. The banks are suitable targets while technology acts a deterrent or capable guardian. Hence, technology can alter the strength of the relationship between cyberfraud and cybersecurity outcomes by acting as a capable guardian. In this case, effective and properly deployed technology will weaken the impact of fraud and vice versa.

Secondly, for the RCT, as technology increases the detection capability or probability may increase depending on the level of deployment, thus making cyberattack more difficult. Here, technology changes the payoff structure of cyberfraud, by influencing the frequency and sophistication of attacks as well as the success rates. The stronger the deployment of technology as a deterrence, the lower the impact of cyberfraud on organisational cybersecurity and vice versa.

The STT and TAM recognise that cybersecurity outcomes are influenced by how well technology is integrated within organisational systems. The moderation logic is that

technology only reduces cyberfraud impact when properly implemented and effectively used by humans and supported by processes within an organisation.

From the four theories, technology can act as a protective moderator (as in RAT), or cost modifier (as in RCT) or as a contextual enabler (as in STT and RAT).

Figure 2 presents the conceptual framework linking the theories to the variables.

Technology as moderator is classified into three types: (1) preventive technologies, (2) detective technologies and (3) responsive technologies.

Table 3 presents the technology-mechanism outcomes (TMO) for the moderation analysis.

In this context, technology is suitable as a moderator since it explains the variation in the strength and direction (when and the conditions in which its effect is stronger or weaker) between cyberfraud perpetration and cybersecurity outcomes.

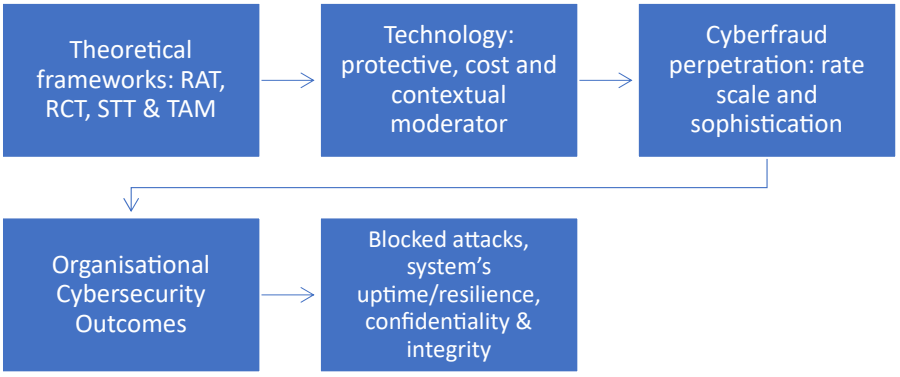

Figure 2. Conceptual framework linking the theories to the variables. Source: Authors' own work

Table 3. Technology-mechanism outcomes (TMO) for the moderation analysis

Technology class	Theoretical mechanism	Measured outcome	Supporting theory
Preventive Technologies: filtering software, firewalls, encryption, virus protection	Target hardening. This empowers organisations to block intrusions	Blocked attacks	RAT
Detective Technologies: intrusion detection systems, automated auditing, discovery sampling, data mining, digital financial ratios, digital analysis and data mining	Risk escalation: Serves as a psychological deterrent by ensuring that the audit trail of perpetrators is visible	Perceived effectiveness of cyberfraud detection leading to system's uptime/ resilience	RCT
Responsive Technologies: incident response and automated recovery	Minimise the impact of cyberfraud risks attack: Bridges the gap between automated alerts and human response or actions	Perceived speed and effectiveness of incidence response and fraud containment: confidentiality, integrity and availability (CIA)	STT
All technology classes	Cognitive adoption path: Promotes compliance via a user-friendly system	Rate of technological adoption and compliance behaviour	TAM

Source(s): Authors' own work

3.1 Dataset

The study adopted a quantitative survey using a questionnaire designed as the survey instrument to obtain a primary dataset from the 17 licensed banks in South Africa. This study is limited to the banking industry in South Africa. The surveyed banks may differ in technological architectures and may face varying cyber-risk exposure, which may make their cybersecurity as well as cyberfraud mitigation outcomes differ substantially. However, the surveyed banks represent the structural diversity and cross-sectional patterns of the banks in South Africa. They share the same regulatory frameworks under the regulation of the South African Reserve Bank and face a similar threat landscape; thus, the findings obtained in this study are indicative of the broader trends in the South African banks. They also embrace the investigated technologies, which makes the outcome of this study generalisable within similar institutional and regulatory frameworks.

Each construct on cyberfraud perpetration, technology and cybersecurity outcomes was designed using the Likert scale format presented in Tables 4–6, respectively. The Tables capture the measurement adapted from the established scales in the literature and modified to suit the study context. The questionnaire was reviewed by experts in the field to ensure content validity. Furthermore, to determine the reliability and internal consistency of the survey items (constructs), the Cronbach's Alpha test was employed. This assesses the accuracy of the questions vis-à-vis the scale of measurement and the subject of investigation to determine their reliability and how closely the set of the constructs are as a group (Cronbach, 1951; Nunnally and Bernstein, 1994). This test is necessary to ascertain if the data gathered from each construct is consistent and can be subject to further analysis. High consistency of the constructs is indicated by a high Cronbach's Alpha value that is close to 1 and vice versa. By the rule of thumb, Cronbach's alpha score of 0.7 and above implies that the survey items are reliable and internally consistent.

Furthermore, convergent validity was ascertained for all factor loadings and the composite reliability values. In addition, the average variance extracted (AVE) values were computed and compared with the limit recommended by Hair *et al*. (2021).

In addition, confirmation of the discriminant validity was established using the heterotrait–monotrait (HTMT) ratio criterion to verify the distinctiveness of the constructs.

Using purposive sampling, specifically the expert sampling method, primary dataset was collected from experts drawn from all 17 banks who are knowledgeable about cyberfraud mitigation. These experts possess the required experience being saddled with managerial responsibilities, cybersecurity and IT management, operations and cyberfraud mitigation. The responses were analysed in the SPSS version 29 environment, leading to the development of a moderation regression model to investigate the moderating impact of technology on cyberfraud perpetration and cybersecurity outcomes in South African banks.

Although data were obtained from experts across the 17 licensed banks in South Africa, the unit of analysis for this study is the individual expert (comprising a minimum of two experts per bank), given the small and uneven number of respondents per bank. This is because the perceptions of cyberfraud and cybersecurity capabilities are characteristically subjective and role-dependent.

Table 4. Frequency table showing the rate of cyberfraud perpetration in the South African banking industry

Rate of cyberfraud perpetration		Frequency	Percent	Valid percent	Cumulative percent
Valid	Rarely	8	19.05	19.05	19.05
	Sometimes	23	54.76	54.76	73.81
	Often	6	14.29	14.29	88.10
	Very Often	5	11.90	11.90	100.00
	Total	42	100.00	100.00	

Source(s): Survey

Table 5. Frequency table showing some anti-fraud technologies adopted in the South African banking industry

		Frequency	Percent	Valid percent	Cumulative percent
Filtering software					
Valid	Ineffective	1	2.40	2.40	2.40
	Effective	18	42.90	42.90	45.20
	Highly effective	23	54.80	54.80	100.00
	Total	42	100.00	100.00	
Firewalls					
Valid	Ineffective	1	2.40	2.40	2.40
	Effective	24	57.10	57.10	59.50
	Highly effective	17	40.50	40.50	100.00
	Total	42	100.00	100.00	
Encryption					
Valid	Ineffective	3	7.10	7.10	7.10
	Not sure	1	2.40	2.40	9.50
	Effective	25	59.50	59.50	69.00
	Highly effective	13	31.00	31.00	100.00
	Total	42	100.00	100.00	
Continuous auditing					
Valid	Ineffective	1	2.40	2.40	2.00
	Effective	22	52.40	52.40	54.80
	Highly effective	19	45.20	45.20	100.00
	Total	42	100.00	100.0	
Discovery sampling					
Valid	Ineffective	4	9.50	9.50	9.50
	Not sure	6	14.30	14.30	23.80
	Effective	18	42.90	42.90	66.70
	Highly effective	14	33.30	33.30	100.00
	Total	42	100.00	100.00	
Virus protection					
Valid	Ineffective	2	4.80	4.80	4.80
	Not sure	1	2.40	2.40	7.10
	Effective	23	54.80	54.80	61.90
	Highly effective	16	38.10	38.10	100.00
	Total	42	100.00	100.00	
Financial ratios					
Valid	Ineffective	3	7.10	7.10	7.10
	Not sure	5	11.90	11.90	19.00
	Effective	15	35.70	35.70	54.80
	Highly effective	19	45.20	45.20	100.00
	Total	42	100.00	100.00	
Digital analysis					
Valid	Ineffective	1	2.40	2.40	2.40
	Not sure	6	14.30	14.30	16.70
	Effective	15	35.70	35.70	52.40
	Highly effective	20	47.60	47.60	100.00
	Total	42	100.00	100.00	
Data mining					
Valid	Ineffective	3	7.10	7.10	7.10
	Not sure	6	14.30	14.30	21.40
	Effective	20	47.60	47.60	69.00
	Highly effective	13	31.00	31.00	100.00
	Total	42	100.00	100.00	

Source(s): Survey

Table 6. Frequency table showing cybersecurity outcomes

		Frequency	Percent	Valid percent	Cumulative percent
Blocked cyberattacks					
Valid	Little extent	2	4.80	4.80	4.80
	Moderate extent	11	26.20	26.20	31.00
	Large extent	29	69.00	69.00	100.00
	Total	42	100.00	100.00	
More uptime					
Valid	No extent	1	2.40	2.40	2.40
	Little extent	3	7.10	7.10	9.50
	Moderate extent	18	42.90	42.90	52.40
	Large extent	20	47.60	47.60	100.00
	Total	42	100.00	100.00	
Confidentiality of information					
Valid	No extent	1	2.40	2.40	2.40
	Little extent	1	2.40	2.40	4.80
	Moderate extent	15	35.70	35.70	40.50
	Large extent	25	59.50	59.50	100.00
	Total	42	100.00	100.00	
Integrity of information					
Valid	No extent	1	2.40	2.40	2.40
	Little extent	1	2.40	2.40	4.80
	Moderate extent	12	28.60	28.60	33.30
	Large extent	28	66.70	66.70	100.00
	Total	42	100.00	100.00	
Availability of information					
Valid	No extent	1	2.40	2.40	2.40
	Little extent	2	4.80	4.80	7.10
	Moderate extent	19	45.20	45.20	52.40
	Large extent	20	47.60	47.60	100.00
	Total	42	100.00	100.00	

Source(s): Survey

The sample comprises 42 respondents within 17 banks (clusters), with 2–3 respondents per bank (mean = 2.47). Considering the probability of within-bank correlation, all regression models were estimated using generalised linear modelling with robust standard errors clustered at the bank level.

3.2 Moderation analysis

Moderation analysis was employed to investigate if there is a change in the strength or direction of the relationship between a predictor variable and a predicted variable vis-à-vis the level of a third variable (moderator) (Baron and Kenny, 1986; Hayes, 2018).

In this study, technology moderates the relationship between cyberfraud perpetrated and cybersecurity outcomes. The focus is on the banks in South Africa, examining cyberfraud perpetrated via phishing, spying, malware, data theft, spamming, online banking fraud, hacking and digital skimming. The mitigating technologies considered include:

(1) Filtering software

(2) Firewalls

(3) Encryption

(4) Automated auditing

(5) Discovery sampling
(6) Virus protection
(7) Digital financial ratios
(8) Digital analysis
(9) Data mining
(10) Incident response and automated recovery

This implies that the impact of cybercrime perpetration may vary depending on the effectiveness of the technology employed. Moderation analysis is suitable in the context of this study because the effect of cybercrime perpetration may vary from one organisation to another depending on the organisation's technological capabilities and cybersecurity systems (Kwon and Johnson, 2014). Secondly, moderation analysis is suitable in testing the interacting effects of independent and dependent variables vis-à-vis a moderator (Hayes, 2018). Hence, technology can impact the effect of cybercrime on cybersecurity outcomes positively or negatively. Rather than examining the linear or direct effect of technology, this study examines its interactive effect with cyberfraud perpetration and cybersecurity outcomes. The use of moderation analysis is appropriate because technological capability may strengthen or weaken the effect of cybercrime on organisational security outcomes rather than exerting only a direct influence (Baron and Kenny, 1986; Hayes, 2018).

The choice of technology as the moderating factor stems from the fact that the information systems theory suggests that an organisation's technological capability level can influence how cyberthreats translate into cybersecurity outcomes (DeLone and McLean, 2003). Empirical cybercrime studies such as Akinbowale *et al*. (2025a, b) also indicate that technologies can influence cybersecurity breach, severity and mitigation (Akinbowale *et al*., 2025a, b). Moderation and interaction analyses are widely used in cybersecurity and information system research to investigate the effect of changes in security controls and technologies on cyber threats (D'Arcy *et al*., 2009; Kwon and Johnson, 2014).

The moderation effect of technology is investigated by examining the interactive effect between the independent variable (cyberfraud perpetration), moderator (technology) and the dependent variable (cybersecurity outcomes) according to the standard moderation regression expressed in Equation (1). Although the responses gathered were in the form of the ordinal Likert-scale format, scales with five or more categories were treated as continuous.

$$Y = \beta_0 + \beta_1 X + \beta_2 M + \beta_3 (X.M) + \varepsilon \tag{1}$$

Where Y denotes the dependent (predicted) variable, X depicts the independent (explanatory) variable, M represents the moderator (which changes the strength or direction of the relationship between X and Y), $X.M$ is the interaction term that depicts the moderation effect, β_0 is the intercept or slope while β_1 represents the key effect of X and Y, keeping M (the moderator) constant, β_2 depicts the effect of M on Y when X is constant, β_3 is the moderator coefficient, which explains how much the effect of X on Y changes for a one-unit increase in M and ε is the residual error, which depicts the proportion of variable Y that is not accounted for by the model.

The moderation analysis follows the following process: definition of variables (X, Y, M), creation of the interaction term, running of the hierarchical regression, test of significance of interaction and Interpretation. The following assumptions underlie the implementation: linearity, normality, homoscedasticity, absence of multicollinearity, independence and reliability of measures.

For the constructs on the deployment of digital technologies (moderator) and cybersecurity outcomes (dependent variable), having nine and five variables, respectively, a composite (construct) score was created. Furthermore, the mean centre was also generated for these

constructs to reduce multicollinearity. The interactive term was also generated as a product of the predictor variable and the moderator. The hierarchical regression was run in two blocks. The first block comprises the main effects of the predictor variable (rate of cyberfraud perpetration) and the moderator (technology) on the predicted variable (cybersecurity outcomes), while the second block comprises of the interactive effect of the predictor variable and the moderator on the predicted variable.

The evaluation of model was done by considering the value of β_3 as well as its p-value. If β_3 assumes a non-zero value, then it implies the presence of a moderating effect. The sign of β_3 indicates whether the effect is positive or negative. Furthermore, a significant model that indicates a strong moderating effect is signaled by a p-value less than 0.05.

4. Results and discussion

4.1 Survey outcomes

Table 4 is the frequency table displaying the rate of cyberfraud perpetration in the South African banking industry with the majority of the respondents (54.76%) indicating that it occurs occasionally. The frequency table of some examples of the anti-fraud technologies deployed to combat cyberfraud is shown in Table 5, while Table 6 is the frequency table showing cybersecurity outcomes.

As shown in Table 6, the cybersecurity outcomes comprise multiple dimensions, such as blocked attacks, system's uptime/resilience, information confidentiality and integrity. These dimensions were combined into a single composite score based on the expert's ratings and were found to be internal consistency as justified by the high Cronbach's alpha value ($\alpha = 0.94$).

4.2 Reliability analysis and discriminant validity

Cybersecurity outcomes, namely threat mitigation (blocked attacks), operational resilience (uptime) and information integrity (CIA), were treated as individual reflective latent constructs because each has a unique set of 5 survey items (Bollen and Lennox, 1991; Jarvis *et al*., 2003).

Furthermore, the cybersecurity outcomes capture an underlying latent dimension rather than a formative index of unrelated outcomes; thus, based on theoretical justification and empirical inter-item correlations, they were treated as a reflective construct. Considering the recommendations of Jarvis *et al*. (2003) and MacKenzie *et al*. (2011), the five items for each of the cybersecurity outcomes (totalling $n = 15$) were parsed into their respective homogeneous groups rather than being collapsed into a single heterogeneous outcome construct.

Table 7 presents the summary of the Cronbach's alpha score per construct. Although a pilot study was not conducted, the reliability analysis carried out indicates that the survey items and their scales of measurement were internally consistent.

Furthermore, convergent validity for all factor loadings was found to be greater than 0.70. The composite reliability values were found to exceed 0.70, and the AVE values were also found to be greater than the recommended minimum value of 0.50 (Hair *et al*., 2021).

In addition, the confirmation of the discriminant validity was achieved using the HTMT ratio criterion (Table 8). The value was found to fall below 0.85, indicating that the constructs are empirically distinct (MacKenzie *et al*., 2011).

4.3 Results obtained from moderation analysis

Table 9 presents the outcome of the correlations among the variables. The correlation indicates the nature of the relationship between the existing pair of independent and dependent variables and is used to determine if they are adequately correlated to justify moderation analysis. The rate of cyberfraud perpetration is denoted by r_c while m_c depicts the moderator (technology) and r_m denotes the interactive variable of r_c and m_c

Table 7. Summary of the construct reliability score per construct

Latent construct name	Variables	*N*	Cronbach's alpha	Composite reliability (CR)	AVE	Factor loadings (range)	Remarks	Reference
Technology	Preventive technologies	9	0.923	0.94 (approx.)	0.66 (approx.)	0.74–0.89	Cronbach's alpha score of 0.923 is high (close to 1). This shows that the construct is reliable and internally consistent and the data garnered from the construct is suitable for further analysis. CR value greater than 0.70 and AVE value greater than 0.50 confirm convergent validity. All item loadings exceed 0.70, indicating strong indicator reliability	Cronbach (1951), Hair *et al.* (2021)
Cybersecurity outcomes	Threat mitigation (measured reflectively by blocked attacks)	5	0.971	0.97 (approx.)	0.87 (approx.)	0.86–0.97	Cronbach's Alpha score of 0.971 is high (close to 1). This shows that the construct is reliable and internally consistent and the data garnered from the construct is suitable for further analysis. CR value greater than 0.70 and AVE value greater than 0.50 confirm convergent validity. High loadings indicate that the construct is a coherent reflective latent variable	Cronbach (1951), Hair *et al.* (2021)
	Operational resilience (measured reflectively by uptime)	5	0.945	0.95 (approx.)	0.88 (approx.)	0.80–0.91	Cronbach's Alpha score of 0.945 is high (close to 1). This shows that the construct is reliable and internally consistent and the data garnered from the construct is suitable for further analysis. CR value greater than 0.70 and AVE value greater than 0.50 confirm convergent validity. High loadings indicate that the construct is a coherent reflective latent variable	Cronbach (1951), Hair *et al.* (2021)
	Information integrity (measured reflectively by confidentiality, integrity and availability)	5	0.928	0.91 (approx.)	0.84 (approx.)	0.82–0.95	Cronbach's Alpha score of 0.928 is high (close to 1). This shows that the construct is reliable and internally consistent and the data garnered from the construct is suitable for further analysis. CR value greater than 0.70 and AVE value greater than 0.50 confirm convergent validity. High loadings indicate that the construct is a coherent reflective latent variable	Cronbach (1951), Hair *et al.* (2021)

Source(s): Authors' computation from field survey data using IBM SPSS Statistics Version 29

Table 8. Discriminant validity using the HTMT criterion

Latent construct	Digital technologies	Threat mitigation	Operational resilience	Information integrity
Deployment of digital technologies	–			
Threat mitigation	0.542	–	–	
Operational resilience	0.603	0.645	–	
Information integrity	0.472	0.501	0.621	–

Source(s): Authors' computation from field survey data using IBM SPSS Statistics Version 29

Table 9. Correlation analysis results

Correlations					
		cybersecurity_score	r_c	m_c	r_m
Pearson correlation	Cybersecurity score	1.000	0.793	−0.443	−0.341
	r_c	0.793	1.000	0.027	−0.136
	m_c	−0.443	0.027	1.000	0.080
	r_m	−0.341	−0.136	0.080	1.000
Sig. (one-tailed)	cybersecurity_score		0.000	0.002	0.014
	r_c	0.000		0.432	0.195
	m_c	0.002	0.432		0.307
	r_m	0.014	0.195	0.307	
N	cybersecurity_score	42	42	42	42
	r_c	42	42	42	42
	m_c	42	42	42	42
	r_m	42	42	42	42

Source(s): Authors' computation from field survey data using IBM SPSS Statistics Version 29

The Table shows that the rate of cybercrime perpetration is positively correlated with the cybersecurity score. This implies that the banks experiencing a high rate of cyberfraud perpetration are also the ones investing more in cybersecurity measures and reporting more controls and vice versa. Conversely, technology deployment and the interactive effect of technology and the rate of cyberfraud perpetration have negative correlations with cybersecurity outcomes. This means an increase in the deployment of technology and the interactive effect may weaken cybersecurity performance. Furthermore, variable r_c is weakly but positively correlated with variable m_c and negatively correlated with the interactive effect (r_m). Variables m_c and r_m are positive but weakly correlated as shown in the table. The variables exhibit positive, negative and fair comparison with each other without the evidence of high multicollinearity, which may affect the outcome of the study. The correlation analysis was assessed using the Pearson Correlation Coefficient.

Table 10 shows the model summary. R measures the correlation between the actual and the predicted values, while R^2 indicates the percentage of variance in the dependent variable accounted for by the independent variable (for this study, 88.3% and 84.5% for the second and first model, respectively). The adjusted R^2 is a measure of fit that indicates the number of predicted values in the model. The closer the values of R, R^2, adjusted R^2 to 1, the better the model and vice versa. The Table shows that for both the first and the second model, their values are close to 1, which indicates that the developed model is robust. Furthermore, the R^2 values were significantly close to the adjusted R^2 values for both models, thus indicating that the model is not overfitted and that the predictor variables are significant.

Table 11 presents the analysis of variance (ANOVA) of the moderation regression model. The results show that the independent variable, moderator and their interaction significantly explain the dependent variable. This is justified by the large F-value and

Table 10. Model's summary

Model summary[c]									
Model	*R*	*R* square	Adjusted *R*-squared	Std. Error of the estimate	Change statistics *R*-squared change	*F* change	df1	df2	Sig. F change
1	0.919[a]	0.845	0.837	0.32718	0.845	106.141	2	39	0.000
2	0.940[b]	0.883	0.874	0.28747	0.038	12.518	1	38	0.001

Note(s): [a]Predictors: (Constant), m_c, r_c, [b]Predictors: (Constant), m_c, r_c, r_m, [c]Dependent Variable: cybersecurity_score

Source(s): Authors' computation from field survey data using IBM SPSS Statistics Version 29

Table 11. Analysis of variance (ANOVA)

ANOVA[a]						
Model		Sum of squares	df	Mean square	F	Sig
1	Regression	22.724	2	11.362	106.141	0.000[b]
	Residual	4.175	39	0.107		
	Total	26.899	41			
2	Regression	23.759	3	7.920	95.830	0.000[c]
	Residual	3.140	38	0.083		
	Total	26.899	41			

Note(s): [a]Dependent Variable: cybersecurity_score, [b]Predictors: (Constant), m_c, r_c, [c]Predictors: (Constant), m_c, r_c, r_m

Source(s): Authors' computation from field survey data using IBM SPSS Statistics Version 29

p-value less than 0.05, which indicate that the regression model has a Good model fit and explains more variance than by random chance.

The coefficients of moderation regression model presented in Table 12 confirms that technology moderated the relationship between cyberfraud perpetration and cybersecurity outcomes. This is justified by the *p*-value less than 0.05 ($0.001 < 0.05$).

For the first model, which investigates the main effects of the predictor variables on the independent variables, the standardised Beta value of β for rate of cyberfraud perpetration was 0.895 while that of technology was −0.190.

For the second model that considers the interaction term (r_m) between the rate of cyberfraud perpetration (denoted as r_c) and technology deployment (m_c) as the predictor variables, the β for rate of cyberfraud perpetration was 0.765, while that of technology was −0.502 and that of the interactive term was −0.430. This also indicates that the banks

Table 12. The coefficients of moderation regression model

Model	Predictor	B	Robust SE	Wald χ^2	*p*-value
1	Constant	3.311	0.155	4.43	0.021
	r_c	0.895	0.130	3.16	0.040
	m_c	−0.190	0.095	4.29	0.034
2	Constant	3.307	0.148	3.09	0.019
	r_c	0.765	0.139	3.35	0.002
	m_c	−0.502	0.021	3.57	0.041
	r × m	−0.430	0.390	10.22	0.000

Source(s): Authors' computation from field survey data using IBM SPSS Statistics Version 29

experiencing a high rate of cyberfraud are also the ones investing more in cybersecurity measures and reporting more controls. The interactive term (denoted as r_m) was statistically significant ($\beta = -0.430, p < 0.05$) indicating that technology moderates the relationship between the rate of cyberfraud perpetration and cybersecurity outcomes. The negative coefficient indicates that as the moderator increases, the effect of the rate of cyberfraud perpetration on cybersecurity outcomes decreases.

The regression model for predicting cybersecurity outcomes (Y) as a function of rate of cyberfraud perpetration (r_c) and technology deployment (m_c) is expressed as Equation (2) while Equation (3) presents the moderated regression model for predicting cybersecurity outcomes as a function of rate of cyberfraud perpetration (r_c), technology deployment (m_c) and the interactive effect (r_m) of r_c and m_c.

$$Y = 3.311 + 0.895\text{r\_c} - 0.19\text{m\_c} \tag{2}$$

$$Y = 3.307 + 0.765\text{r\_c} - 0.502\text{m\_c} - 0.430\text{r\_m} \tag{3}$$

Equation (2) indicates that for a one-unit increase in the rate of cyberfraud perpetration, cybersecurity outcomes increase by 0.895 units, holding technology deployment constant, while for the second model, a one-unit increase in technology deployment results in a decrease of 0.430 units in cybersecurity outcomes, holding the rate of cyberfraud perpetration constant.

For the second model, a one-unit increase in the interactive term leads to a decrease in cybersecurity outcomes by 0.430 units, holding other variables constant. The negative interaction in Equations (2) and (3) means that the slope of cyberfraud and cybersecurity outcomes changes with technology. This implies that the positive slope becomes weaker as technology increases.

This result implies that although cyberfraud perpetration propels the banking institutions to improve their cybersecurity. The second model (Equation (3)) shows that as technology deployment increases, the strength of the positive effect achieved with the first model reduces. Hence, technology moderates the relationship by reducing the effect of cyberfraud perpetration on cybersecurity at high technological levels. This further implies that small banks may witness a lower rate of cyberfraud perpetration, requiring fewer cybersecurity systems, while large banks may be prone to a higher rate of cyberfraud perpetration, requiring an increase in cybersecurity systems. While the rate of cyberfraud perpetration generally increases cybersecurity outcomes or measures, the deployment of technology changes the strength of this relationship. For banks with a higher level of technology, the positive impact of cyberfraud on cybersecurity may be weaker compared to low-level organisations. This may be because high technologically driven banks may already have some state-of-the-art cybersecurity, hence cyberbreach or an increasing rate of cyberfraud perpetration may have a less positive and significant effect.

Table 13 shows the moderating effects of technology types on cyberfraud perpetration. The analysis is structured into two models. The first model investigates the direct effects of disaggregated technology constructs (preventive, detective and response) alongside the main predictor, while the second model introduces the interaction terms to test their moderating roles within a unified framework. This is to allow for comparison analysis of the unique effects of different technology types.

The overall moderated model (Equation (4)) shows that while cyberfraud perpetration significantly increases cybersecurity outcomes adversely.

The intercept (2.465) denotes the expected cybersecurity outcome when all variables are at their mean, while the main effect of cyberfraud perpetration (0.371) implies that a unit increase in cyberfraud perpetration may lead to an increase in negative cybersecurity outcomes by +0.371. This effect is strong and harmful.

For the direct effect of technologies, the results show that the rate of cyberfraud perpetration has a positive and significant effect on cybersecurity outcomes (β = 0.450,

Table 13. Moderating effects of technology types on cyberfraud perpetration

Variables	Model 1 (main effects) B (SE)	Model 2 (moderation) B (SE)	Wald χ^2	*p*-value
Constant	2.640 (0.230)	2.465 (0.235)	121.32	0.000
(r_c)	0.450 (0.135)	0.371 (0.136)	6.92	0.005
Preventive ($prev_c$)	−0.880 (0.160)	−0.249 (0.122)	3.69	0.031
Detective (det_c)	−0.640 (0.132)	−0.334 (0.240)	2.91	0.024
Response ($resp_c$)	−0.075 (0.081)	−0.079 (0.095)	0.54	0.240
r × Preventive	–	−0.223 (0.102)	2.84	0.032
r × Detective	–	−0.270 (0.110)	3.02	0.024
r × Response	–	0.124 (0.055)	1.29	0.128

Source(s): Authors' computation from field survey data using IBM SPSS statistics version 29

$p < 0.05$), implying that an increase in cyberfraud activities may be associated with worse cybersecurity outcomes.

For the deployment of preventive technologies ($\beta = -0.880$, $p < 0.05$) and detective technologies ($\beta = -0.640$, $p < 0.05$), there were significant reductions in negative cybersecurity outcomes. The detective technologies, however, show stronger reduction capability. Conversely, the response technologies indicate a weak effect and are not statistically significant ($\beta = -0.075$, $p > 0.05$), thus implying limited direct effectiveness.

The preventive moderation has a coefficient of −0.223, which implies that an increase in preventive technologies reduces the effect of cyberfraud thereby buffering cyberfraud impact. Similarly, the detective moderation shows the strongest buffering effect with a coefficient of −0.270, indicating that detective technologies significantly weaken the impact of cyberfraud perpetration. Lastly, the response moderation has a coefficient of +0.124 (positive but not significant), suggesting that the response strategies may not effectively mitigate the impact of cyberfraud perpetration.

While the preventive and especially the detective technologies significantly mitigate cyberfraud perpetration effect, the response technologies exhibit no significant buffering role, thus indicating limited effectiveness.

From Table 13, the overall moderated equation becomes Equation (4).

$$Y = 2.465 + 0.371\mathrm{r_c} - 0.249\mathrm{prev_c} - 0.3340\mathrm{det_c} - 079\mathrm{resp_c} - 0.223(\mathrm{r_c} * \mathrm{prev_c}) - 0.270(\mathrm{r_c} * \mathrm{det_c}) + 0.124(\mathrm{r_c} * \mathrm{resp_c}) + \varepsilon \quad (4)$$

Table 14 presents the collinearity diagnostics of the moderation regression model. Eigenvalues reveal how much variance is explained by each dimension, while the condition index indicates how stable the model is. The variance proportions indicate the amount of variance of each variable associated with a specific dimension. According to the results shown in Table 14, large eigenvalues that are not close or approximately zero were obtained, which indicates the absence of linear dependence among the predictor variables. In addition, condition indices were less than 10, which indicates that the model is stable, coupled with the fact that the variance proportion did not indicate shared variance among the predictor variables in any single dimension.

Table 15 shows the residual statistics of the moderation regression model. The residual is the error of prediction that shows the difference between the actual and predicted values of the dependent variables. The residuals were normally distributed with a mean value of 0.000 (Table 15), which indicates a perfect agreement between the actual and predicted values.

Figure 3 shows the normal plot of the regression residual, showing that the residuals were normally distributed with the mean close to zero with few outliers. The scatter plot showed no

Table 14. Collinearity diagnostics of the moderation regression model

Collinearity diagnostics[a]							
				Variance proportions			
Model	Dimension	Eigenvalue	Condition index	(Constant)	r_c	m_c	r_m
1	1	1.027	1.000	0.00	0.49	0.49	
	2	1.000	1.014	1.00	0.00	0.00	
	3	0.973	1.028	0.00	0.51	0.51	
2	1	1.151	1.000	0.02	0.31	0.07	0.45
	2	1.024	1.060	0.02	0.25	0.69	0.01
	3	0.998	1.074	0.94	0.01	0.05	0.00
	4	0.826	1.180	0.02	0.42	0.20	0.54

Note(s): [a]Dependent Variable: cybersecurity_score

Source(s): Authors' computation from field survey data using IBM SPSS statistics version 29

Table 15. Residual statistics

Residuals statistics[a]					
	Minimum	Maximum	Mean	Std. Deviation	*N*
Predicted Value	1.2000	5.4779	4.4381	0.76124	42
Residual	−1.10033	0.33168	0.00000	0.27676	42
Std. Predicted Value	−4.254	1.366	0.000	1.000	42
Std. Residual	−3.828	1.154	0.000	0.963	42

Note(s): [a]Dependent Variable: cybersecurity_score

Source(s): Authors' computation from field survey data using IBM SPSS statistics version 29

evidence of heteroscedasticity, which shows a goodness fitness of the model and the fact that the error changes are constant as the predictor changes.

Figure 4 display the scatter plot of the regression model. The figure shows that the data points are randomly scattered, with approximately equal spread above and below 0 with no specific pattern or shape. This indicates that the error variance is approximately constant and the relationship of the variables is linear, thus satisfying the regression model's assumption. It further implies that the output of the regression model is reliable.

Figures 5–7 show the partial plot of the impact of dependent variables, namely the rate of cyberfraud perpetration, technology deployment and their interactive effect on cybersecurity outcomes, respectively. Figure 5 shows a straight-line pattern, thus satisfying the linearity assumption. The upward trend shows the direction of the relationship, indicating a positive partial effect, while the strength of the relationship is shown by the tight clustering of the data points along the diagonal line, which indicates that the rate of cyberfraud perpetration is a strong predictor of cybersecurity outcomes.

Figure 6 shows a straight-line pattern, thus satisfying the linearity assumption. The downward trend shows a negative direction of the partial effect, indicating that technology deployment has a negative relationship with cybersecurity outcomes. The strength of the relationship is revealed by the scattered data points along the diagonal line, which indicates that technology deployment is a weak predictor of cybersecurity outcomes.

Figure 7 shows a straight-line pattern, thus satisfying the linearity assumption. The downward trend shows a negative direction of the partial effect, indicating that technology deployment has a negative relationship with cybersecurity outcomes. The strength of the relationship is revealed by the clustered data points along the diagonal line, which indicates that the interactive term is a strong predictor of cybersecurity outcomes.

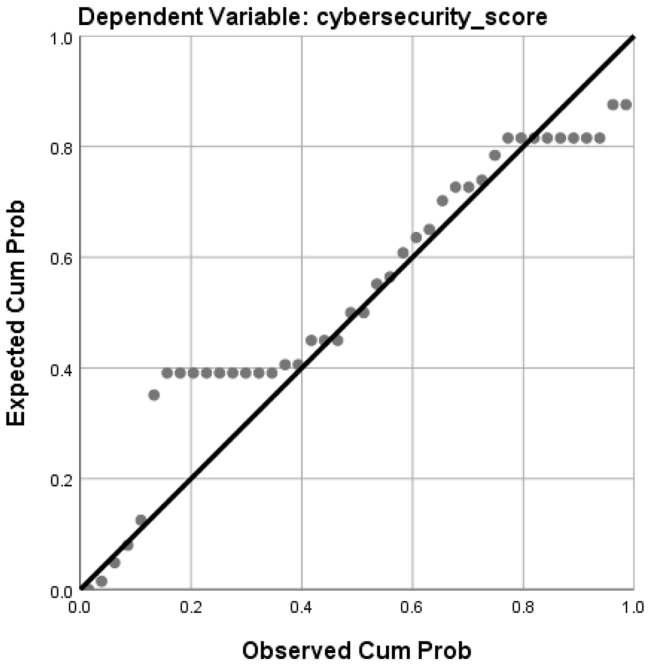

Figure 3. The normal P-P plot of regression standardised residual. Source: Generated by authors from field survey data analysed using IBM SPSS Statistics version 29

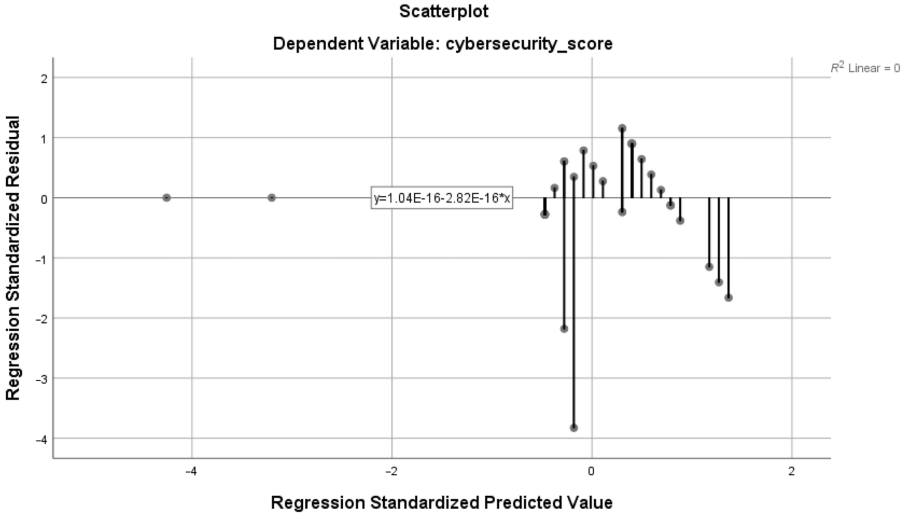

Figure 4. The scatter plot of the regression model. Source: Generated by authors from field survey data analysed using IBM SPSS Statistics version 29

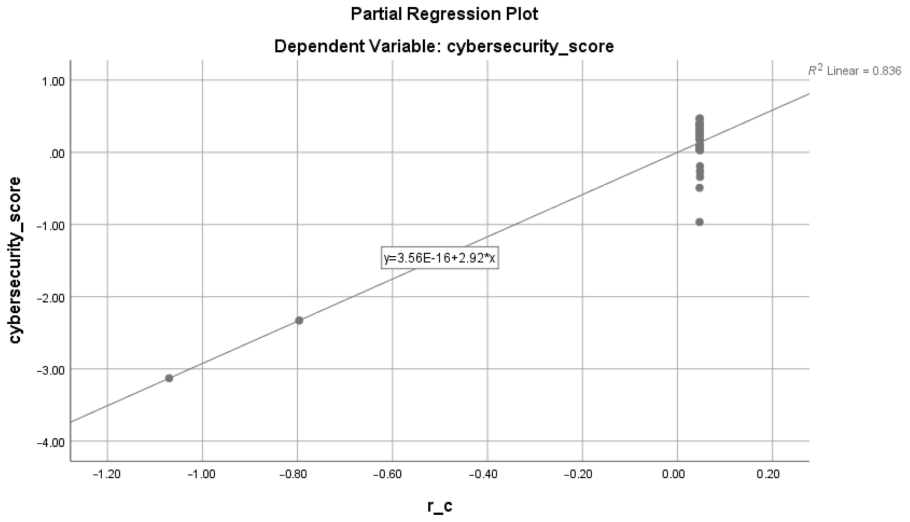

Figure 5. The partial plot of the impact of the rate of cyberfraud perpetration on cybersecurity outcomes. Source: Generated by authors from field survey data analysed using IBM SPSS Statistics version 29

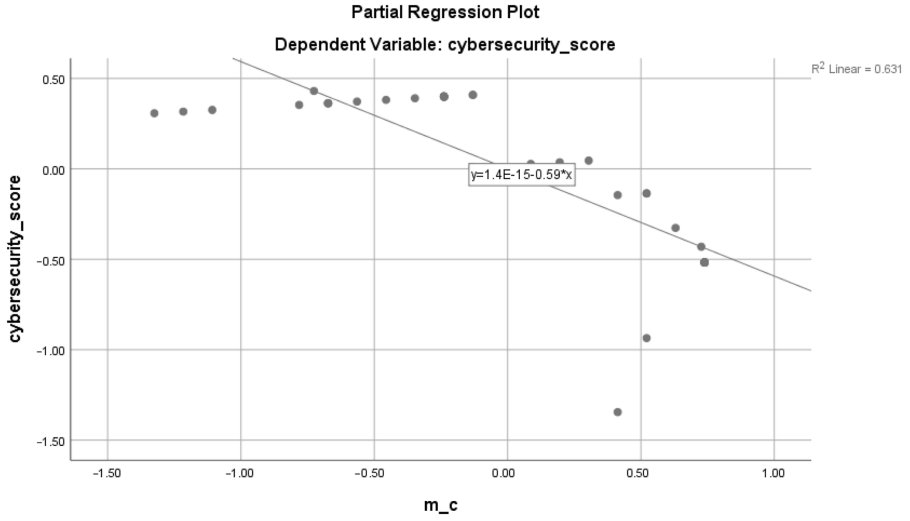

Figure 6. The partial plot of the impact of technology on cybersecurity outcomes. Source: Generated by authors from field survey data analysed using IBM SPSS statistics version 29

4.4 Discussion of results

The moderation analysis indicates three major findings. First, the rate of cyberfraud perpetration has a statistically significant influence on cybersecurity outcomes. This suggests that the banks experiencing a high rate of cyberfraud perpetration are also the ones investing more in cybersecurity measures and reporting more controls and vice versa. Secondly, the moderator, technology deployment, has a negative and weak influence on cybersecurity outcome.

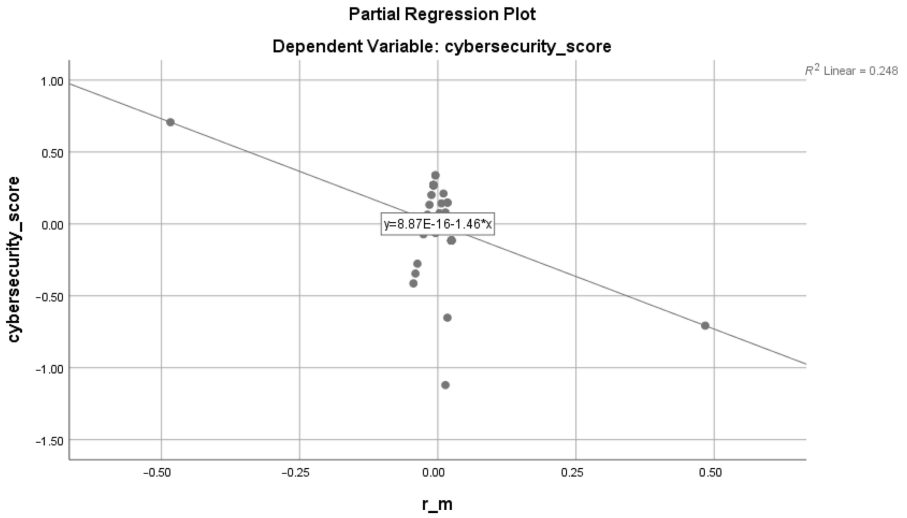

Figure 7. The partial plot of the iterative effect of the rate of cyberfraud perpetration and technology on cybersecurity outcomes. Source: Generated by authors from field survey data analysed using IBM SPSS Statistics version 29

Third, by moderating with technology, the results show that the interactive term has a negative and significant influence on cybersecurity outcomes. Hence, the outcome of the interaction term between cyberfraud perpetration and organisation's technological ability is statistically significant and negative ($\beta = -1.462$, $p < 0.05$). This indicates that technology moderates the relationship between cyberfraud perpetration and organisation's security outcomes.

The significant influence of the rate of cybercrime perpetration on cybersecurity outcomes indicates banks experiencing a high rate of cyberfraud perpetration are also the ones investing more in cybersecurity measures and reporting more controls and vice versa. This is because increased cyberattack could propel the banks to strengthen their cybersecurity systems. Banks may tighten their security measures or invest more in cybersecurity in response to cyberattacks in line with the reactive security strategy, which notes that organisations may respond reactively to increasing cybersecurity incidents rather than measure them proactively (Anderson *et al*., 2019). As cyberattacks increase, cybersecurity awareness may also increase, coupled with investment in cybersecurity infrastructure, policies and training. This finding agrees with Kshetri (2010), who found that cybercrime incidents could drive organisations and governments to develop and implement a more robust security system. Similarly, Gordon *et al*. (2021) stated that organisations experiencing incessant attacks may spend more on cybersecurity. The RAT also supports this finding that increased cybercrime can increase the perceived risk, thus motivating the guardianship to implement stronger cybersecurity measures (Holt and Bossler, 2014). However, this finding is refuted by Herath and Rao (2009), who argue that increased cyberattacks may weaken an organisation's cybersecurity measures and compliance with standards. Nonetheless, this current finding indicates that the overall increasing rate of cyberfraud perpetration may strengthen cybersecurity measures.

The outcome of this study further shows that technology has a negative and weak influence on cybersecurity. This suggests that advancement in technology may not guarantee robust cybersecurity, as it may worsen it in some cases. Technology deployment is usually perceived as a "two-edged sword" by enabling digital transformation and advanced security solutions, yet it can also increase organisation system's vulnerability to cyberattacks, thus creating

opportunities for threat actors (Böhme and Moore, 2016). Lin *et al*. (2017) stated that the use of technologies such as cloud computing, AI, etc. without a strong security integration may weaken cybersecurity outcomes. Similarly, Dhillon and Backhouse (2001) stated that increasing technological innovation without corresponding security controls may increase vulnerabilities. However, Venkatesh *et al.* (2012) argue that technology adoption, when matched with user competence, can promote system security. Thus, technology, in isolation, may not sufficiently promote cybersecurity. There is a need for robust cybersecurity measures, adequate governance, user competence and expertise.

The moderating effect of technology demonstrated in this study indicates that as technology increases, the positive effect of cybercrime occurrence on cybersecurity may reduce. This finding shows that while cyberfraud perpetration may lead to reinforcement of an organisation's cybersecurity architecture, the use of advanced technologies without the required expertise may hinder an effective security response. This calls for human training on the emerging and digital anti-fraud technology implementation. Some organisations may have advanced security solutions that are technologically driven, but without an expert who can implement them, the potential of such technologies may be sub-optimally harnessed, thus slowing down the effectiveness of organisation's response to cyberattacks. Siponen and Oinas-Kukkonen (2007) noted that technological advancement or complexity can overwhelm users and security personnel, reducing the efficiency of cybersecurity measures amidst cyberthreats, even in the face of increasing cyber threats. Brenner (2011) also stated that threat actors often exploit advanced technologies faster than defenders can utilise or secure them. Therefore, as cyberfraud perpetration increases, banks that depend heavily on technology must implement adequate security and effectively integrate it into the existing security architecture while ensuring user competence at organisation's level. This is necessary to effectively translate technological solutions into positive cybersecurity outcomes. This finding contradicts studies such as Shackelford *et al*. (2014) that perceive technology such as automation, AI, etc. as a major enabler of adaptive cybersecurity. Other critical factors such as technological readiness, human expertise and regulatory frameworks should also be considered.

These findings indicate that cybersecurity is not solely a function of cyber threats or technological advancement but of how technology is managed or effectively deployed. Technology should be effectively integrated into security strategies in alignment with capacity building and governance to ensure that it will play a positive role in cybersecurity rather than weakening it.

These findings align with the theoretical frameworks of RAT, RCT, STT and TAM underpinning this work. The moderating effect of technology demonstrated in this study shows that it can act as a capable guardian if properly configured and utilised. This can reduce the opportunity of the threat actors to commit fraud in line with the RAT of fraud. On the other hand, if poorly configured or utilised, it could also increase fraud opportunities and worsen cybersecurity outcomes. In the context of RCT, findings revealed that if properly configured and utilised, it could increase the risk and cost of cyberfraud perpetration. However, if properly configured and utilised, attackers may exploit the loopholes, thereby unintentionally reducing the perceived risk and cost cyberfraud perpetration. In terms of the STT, alignment of the deployed technology with human capabilities, organisational process and user behaviour can promote cybersecurity outcomes, while misalignment may lead to system's failure and increased cyberfraud risk.

The banking industry and other financial institutions can operationalise these findings in practice via the development of integrated cybersecurity governance frameworks. For instance, they can invest in preventive technologies such as firewalls and end-to-end encryption, detective technologies such as intrusion detection systems, AI-based monitoring tools for automated auditing and real-time transaction screening as well as responsive technologies such as incident response and automated recovery.

4.5 Answering research questions and hypothesis validation

Moderation occurs when there is a change in the strength or direction of the relationship between an independent variable and a dependent variable via the introduction of a third variable called the moderating variable. In this study, technology serves as a moderating variable that alters how cyberfraud perpetration influences cybersecurity.

4.5.1 How does technology moderate the relationship between cyberfraud perpetration and organisation cybersecurity outcomes?. The results obtained indicated that cyberfraud perpetration generally leads to reinforcement of an organisation's cybersecurity architecture as a reactive measure. Technology as a moderating variable changes this relationship by altering the suitability of the target and the guardianship in line with the RAT (Cohen and Felson, 1979). The interactive term of the moderator gave a negative but significant relationship between cyberfraud occurrence and cybersecurity. This suggests that the deployment of advanced technologies can introduce new vulnerabilities or weaken cybersecurity due to complexity, leading to more cyberattacks. Furthermore, where the required technical expertise to drive the digital technologies is lacking, organisations may not be able to respond effectively to cyberthreats. This implies that organisations adopting more advanced technologies, without enabling expertise and supporting governance and infrastructure, may reduce their ability to translate cyberfraud experiences into effective cybersecurity improvements.

4.5.2 What is the moderating impact of technology on cyberfraud perpetration and organisation cybersecurity outcomes?. In answering the second research question, the negative and significant interaction term shows that technology weakens the positive influence of cyberfraud perpetration on cybersecurity.

Equation (3) shows that a one-unit increase in the interactive term leads to a decrease in cybersecurity outcomes by 0.430 units, holding other variables constant. This result implies that cyberfraud perpetration propels banks to improve their cybersecurity. Furthermore, the slope of cyberfraud and cybersecurity outcomes changes with technology and the negative interaction means the positive slope becomes weaker as technology increases. Hence, technology moderates the relationship by reducing the effect of cyberfraud perpetration on cybersecurity at high technological levels.

4.5.3 Hypothesis validation. The hypothesis (H_1) states that "H_1: Preventive, detective, and response technologies significantly weaken the negative relationship between cyberfraud perpetration and cybersecurity outcomes".

The results presented in Table 13 indicate that while the preventive and especially the detective technologies significantly moderate and mitigate cyberfraud perpetration effect, the response technologies exhibit no significant buffering role, thus indicating limited effectiveness.

Table 16 captures the hypothesis validation.

Table 16. Hypothesis validation

Technology type	Moderation effect	Decision	Remarks
Preventive	Negative and significant moderation	Accept H_1 and reject H_0	Reduces impact early
Detective	Negative and significant moderation	Accept H_1 and reject H_0	Demonstrate effective control
Response	Not significant	Fail to reject H_0	Limited post event resilience

Source(s): Authors' own work

5. Conclusion and policy recommendations

This study conducted a quantitative survey using questionnaire as the survey instrument to obtain a primary dataset from the 17 licensed banks in South Africa. It draws insights from the criminological and information systems theories to determine the moderating role of technology in the relationship between cyberfraud occurrence and cybersecurity outcomes. Moderation analysis carried out in the SPSS version 29 environment indicates three major findings.

From the outcome of this study, the following are some policy recommendations that can assist the banking institution to optimally harness the potential of technology to enhance cybersecurity:

(1) First, the significant relationship between cyberfraud perpetration and cybersecurity suggests that the banks are still reactionary than being proactive. Hence proactive responses may be formulated and implemented to promote cyber-resilience and reduce reactionary measures triggered by cyberattacks.

(2) The strong negative effect of the moderating term suggests that technology adoption often occurs without sufficient cyber-security integration. Therefore, regulators may ensure that the minimum requirement for the adoption and implementation of these technologies is met and an impact assessment of these technologies should be conducted regularly.

(3) The use of advanced technologies must be matched with the required expertise to promote an effective security response. This calls for human training on emerging and digital anti-fraud technology implementation.

(4) Banks which depend heavily on technology must implement adequate security and effectively integrate them into their security architecture while ensuring user competence at organisation's level. This is necessary to effectively translate technological solutions into positive cybersecurity outcomes.

(5) Technology should be adopted in alignment with capacity building and effective governance to ensure that it will play a positive role in cybersecurity rather than weakening it.

Cyberfraud is a transnational phenomenon that affects financial systems across continents, including Africa, Europe, Asia and the Americas. These findings may inform cybersecurity strategies and technological governance frameworks in financial institutions operating in different regulatory and technological environments. For instance, the outcome of this study could contribute to global discussions on digital banking security, financial technology regulation and cross-border cybercrime prevention.

The findings may support the development of policies that encourage financial institutions globally to strengthen technological capability, invest in cybersecurity infrastructure, and adopt standardised risk management frameworks for cyberfraud prevention. Policymakers, regulators, Central Banks and financial supervisory authorities across the world may apply the outcome of this study to design regulatory guidelines, cybersecurity compliance requirements and collaborative cyber threat intelligence systems.

This study is limited to a quantitative survey covering the 17 licensed banks in South Africa; future studies can explore a mixed approach and extend the investigation to other institutions or organisations that are liable to cyberattack. In addition, future studies can also explore other variables that can moderate the relationship between cyberfraud perpetration such as level of awareness, organisation's culture, governance, regulatory framework, user awareness, cybersecurity investment levels, etc. Further studies could examine industries beyond banking, compare technological capabilities across countries or investigate emerging technologies such as AI, blockchain and behavioural analytics to mitigate cyberfraud. Comparative or cross-continental studies would be particularly valuable for understanding

how technological interventions influence cybersecurity outcomes across different institutional and regulatory contexts. Finally, future studies may further strengthen the survey instrument via formal pilot testing and cognitive interviews.

References

Adewopo, V.A., Azumah, S.W., Yakubu, M.A., Gyamfi, E.K. and Elsayed, N. (2025), "Comprehensive analytical review of cybercrime and cyber policy in West Africa", *Journal of Electrical Systems and Information Technology*, Vol. 12 No. 1, 20, doi: 10.1186/s43067-025-00216-x

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2023), "Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation", *Cogent Economics and Finance*, Vol. 11 No. 1, 2153412, doi: 10.1080/23322039.2022.2153412.

Akinbowale, O.E., Zerihun, M.F. and Mashigo, P. (2024), "Application of situational crime prevention framework for cybercrime mitigation", *International Journal of Cyber Behavior, Psychology and Learning*, Vol. 14 No. 1, pp. 1-23.

Akinbowale, O.E., Zerihun, M.F. and Mashigo, P. (2025a), "impact of legal framework on cyberfraud perpetration in the South African banking industry", *International Journal of Management and Sustainability*, Vol. 14 No. 1, pp. 143-160, doi: 10.18488/11.v14i1.4036.

Akinbowale, O.E., Klingelhöfer, H.E., Zerihun, M.F. and Mashigo, P. (2025b), "Emerging technologies as a mediating factor between causes of cyberfraud and cyberfraud perpetration in the South African banking industry", *International Journal of Cyber Behavior, Psychology and Learning*, Vol. 15 No. 1, pp. 1-19, doi: 10.4018/IJCBPL.378306.

Akujobi, C., Ogwueleka, F., Aimufua, G. and Bassey, S. (2026), "Cyber fraud in Nigerian banks: trends, regulatory gaps, and mitigation strategies (2020-2025)", *Engineering and Technology Journal*, Vol. 11 No. 01, pp. 8575-8580, doi: 10.47191/etj/v11i01.18.

Ali, M.A., Azad, M.A., Centeno, M.P., Hao, F. and van Moorsel, A. (2019), "Consumer-facing technology fraud: economics, attack methods and potential solutions", *Future Generation Computer Systems*, Vol. 100, pp. 408-427, doi: 10.1016/j.future.2019.03.041.

Ali, A., Shah, M., Foster, M. and Alraja, M.N. (2025), "Cybercrime resilience in the era of advanced technologies: evidence from the financial sector of a developing country", *Computers*, Vol. 14 No. 2, p. 38, doi: 10.3390/computers14020038.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganan, C.H., Grasso, T., Levi, M., Moore, T. and Vasek, M. (2019), "Measuring the changing cost of cybercrime", *The 2019 Workshop on the Economics of Information Security*, Boston.

Aphane, M.P. (2023), "Cybersecurity awareness on cybercrime among the youth in Gauteng province", *International Journal of Social Science Research and Review*, Vol. 6 No. 8, pp. 23-32, doi: 10.47814/ijssrr.v6i8.1414.

Baron, R.M. and Kenny, D.A. (1986), "The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations", *Journal of Personality and Social Psychology*, Vol. 51 No. 6, pp. 1173-1182, doi: 10.1037/0022-3514.51.6.1173.

Böhme, R. and Moore, T. (2016), "The 'Iterated Weakest Link' model of adaptive security investment", *Journal of Information Security*, Vol. 7 No. 02, pp. 81-102, doi: 10.4236/jis.2016.72006.

Bollen, K. and Lennox, R. (1991), "Conventional wisdom on measurement: a structural equation perspective", *Psychological Bulletin*, Vol. 110 No. 2, pp. 305-314, doi: 10.1037/0033-2909.110.2.305.

Brenner, J. (2011), *America the Vulnerable: inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, Penguin Press, Ney York.

Buczak, A.L. and Guven, E. (2016), "A survey of data mining and machine learning methods for cyber security intrusion detection", *IEEE Communications Surveys and Tutorials*, Vol. 18 No. 2, pp. 1153-1176, doi: 10.1109/COMST.2015.2494502.

Bukhari, M., Sattar, S., Saleem, S., Khan, K.Z. and Khan, A. (2024), "The impact of cybercrime incidents and artificial intelligence adoption on organizational performance: a mediation and moderation model", *Journal of Excellence in Social Sciences*, Vol. 3 No. 3, pp. 191-210.

Button, M. and Cross, C. (2017), *Cyber Frauds, Scams and their Victims*, Routledge, London, doi: 10.4324/9781315679877.

Chen, J., Henry, E. and Jiang, X. (2023), "Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach", *Journal of Business Ethics*, Vol. 187 No. 1, pp. 199-224, doi: 10.1007/s10551-022-05107-z.

Cohen, L.E. and Felson, M. (1979), "Social change and crime rate trends: a routine activity approach", *American Sociological Review*, Vol. 44 No. 4, pp. 588-608, doi: 10.2307/2094589.

Cronbach, L.J. (1951), "Coefficient alpha and the internal structure of tests", *Psychometrika*, Vol. 16 No. 3, pp. 297-334, doi: 10.1007/BF02310555.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, pp. 319-340, doi: 10.2307/249008.

DeLone, W.H. and McLean, E.R. (2003), "The DeLone and McLean model of information systems success: a ten-year update", *Journal of Management Information Systems*, Vol. 19 No. 4, pp. 9-30, doi: 10.1080/07421222.2003.11045748.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153, doi: 10.1046/j.1365-2575.2001.00099.x.

D'Arcy, J. and Herath, T. (2011), "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", *European Journal of Information Systems*, Vol. 20 No. 6, pp. 643-658, doi: 10.1057/ejis.2011.23.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98, doi: 10.1287/isre.1070.0160.

ENISA (2022), *ENISA Threat Landscape Report 2022*, European Union Agency for Cybersecurity, available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf (accessed 30 March 2026).

Firdaus, R., Xue, Y., Gang, L. and Ali, M.S. (2022), "Artificial intelligence and human psychology in online transaction fraud", *Frontiers in Psychology*, Vol. 13, 947234, doi: 10.3389/fpsyg.2022.947234.

Gordon, L.A. and Loeb, M.P. (2002), "The economics of information security investment", *ACM Transactions on Information and System Security*, Vol. 5 No. 4, pp. 438-457, doi: 10.1145/581271.581274.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2021), "Investing in cybersecurity: insights from the Gordon–Loeb model", *Journal of Information Security*, Vol. 7 No. 2, pp. 49-59, doi: 10.4236/jis.2016.72004.

Greitzer, F.L. and Frincke, D.A. (2010), "Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation", *Insider Threats in Cyber Security*, pp. 85-113, doi: 10.1007/978-1-4419-7133-3_5.

Hadnagy, C. (2018), *Social Engineering: the Science of Human Hacking*, 2nd ed., Wiley, NJ, doi: 10.1002/9781119433729.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2021), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed., SAGE Publications, Thousand Oaks CA.

Hayes, A.F. (2018), *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-based Approach*, 2nd ed., Guilford Press, New York.

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165, doi: 10.1016/j.dss.2009.02.005.

Holt, T.J. and Bossler, A.M. (2014), "An assessment of the current state of cybercrime scholarship", *Deviant Behavior*, Vol. 35 No. 1, pp. 20-40, doi: 10.1080/01639625.2013.822209.

Jarvis, C.B., MacKenzie, S.B. and Podsakoff, P.M. (2003), "A critical review of construct indicators and measurement model misspecification in marketing and consumer research", *Journal of Consumer Research*, Vol. 30 No. 2, pp. 199-218, doi: 10.1086/376806.

Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. and Kirda, E. (2019), "UNVEIL: a large-scale, automated approach to detecting ransomware", *USENIX Security Symposium*, available at: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kharraz.pdf (accessed 30 March 2026).

Kritzinger, E. and von Solms, S.H. (2012), "A framework for cyber security in Africa", *Journal of Information Assurance and Cybersecurity*, pp. 1-10, 322399, doi: 10.5171/2012.322399

Kshetri, N. (2010), *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Springer-Verlag Berlin Heidelberg, doi: 10.1007/978-3-642-11522-6.

Kwon, J. and Johnson, M.E. (2014), "Proactive versus reactive security investments in the healthcare sector", *MIS Quarterly*, Vol. 38 No. 2, pp. 451-471, doi: 10.25300/misq/2014/38.2.06.

Levi, M. and Smith, R.G. (2021), "Fraud and its relationship to pandemics and economic crises: from Spanish flu to COVID-19", *AIC reports Research Report*, Vol. 19, pp. 1-74, available at: https://www.aic.gov.au/sites/default/files/2021-04/rr19_fraud_and_its_relationship_to_pandemics_and_economic_crises.pdf

Li, L., Xu, L. and He, W. (2022), "The effects of antecedents and mediating factors on cybersecurity protection behavior", *Computers in Human Behavior*, Vol. 5, 100165, doi: 10.1016/j.chbr.2021.100165.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W. (2017), "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications", *IEEE Internet of Things Journal*, Vol. 4 No. 5, pp. 1125-1142, doi: 10.1109/JIOT.2017.2683200.

MacKenzie, S.B., Podsakoff, P.M. and Podsakoff, N.P. (2011), "Construct measurement and validation procedures in mis and behavioral research: integrating new and existing techniques", *MIS Quarterly*, Vol. 35 No. 2, pp. 293-334, doi: 10.2307/23044045.

Maluleke, W. (2023), "Exploring cybercrime: an emerging phenomenon and associated challenges in Africa", *International Journal of Social Science Research and Review*, Vol. 6 No. 6, pp. 223-243, doi: 10.47814/ijssrr.v6i6.1360.

Matsaung, P.M. (2023), "An exploration of the use of intelligence-led policing in combating cybercrimes in South Africa", (Unpublished master's thesis), University of South Africa, available at: https://hdl.handle.net/10500/31388

Mushtaq, S. and Shah, M. (2024), "Critical factors and practices in mitigating cybercrimes within e-government services: a rapid review on optimising public service management", *Information*, Vol. 15 No. 10, p. 619, doi: 10.3390/info15100619.

Mushtaq, S. and Shah, M. (2025), "Mitigating cybercrimes in e-government services: a systematic review and bibliometric analysis", *Digital*, Vol. 5 No. 1, p. 3, doi: 10.3390/digital5010003.

Nunnally, J.C. and Bernstein, I.H. (1994), *Psychometric Theory*, 3rd ed., Mc Graw Hill, New York.

Nwafor, I.E. (2024), "Cybercrime investigation and prosecution in Nigeria: bridging the gaps", *African Journal of Legal Studies*, Vol. 16 No. 3, pp. 249-270, doi: 10.1163/17087384-12340108.

Olanrewaju, O.M. and Adebiyi, F.O. (2014), "The impact of mobile information and communication technology on cybercrime in Nigeria", *International Journal of Engineering Research and Technology*, Vol. 3 No. 8, pp. 586-595.

Ransbotham, S. and Mitra, S. (2013), "The impact of immediate disclosure on attack diffusion and volume", in Schneier, B. (Ed.), *Economics of Information Security and Privacy III*, Springer, New York, NY, doi: 10.1007/978-1-4614-1981-5_1.

Romanosky, S., Ablon, L., Kuehn, A. and Jones, T. (2019), "Content analysis of cyber insurance policies: how do carriers price cyber risk?", *Journal of Cybersecurity*, Vol. 5 No. 1, tyz002, doi: 10.1093/cybsec/tyz002.

Saidi, I.C., Kimuyu, J.J. and Handa, S. (2024), "The implications of cybercrime on economic security: the case of Kenya", *International Journal of Research and Innovation in Social Science*, Vol. 8 No. 9, pp. 2464-2471, doi: 10.47772/IJRISS.2024.8090204.

Setona, M.M. (2024), "An exploration of the role of SAPS forensic experts in cyber-crime investigations in Tshwane, Gauteng", (Unpublished dissertation), University of South Africa, available at: https://uir.unisa.ac.za/items/091bd607-30ae-4c02-87f3-64c4fac299cc

Shackelford, S.J., Proia, A.A., Martell, B. and Craig, A.N. (2014), "Toward a global cybersecurity standard of care? Exploring the implications of the 2014", *NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, available at: https://hdl.handle.net/10535/10244

Siponen, M. and Oinas-Kukkonen, H. (2007), "A review of information security issues and respective research contributions", *ACM SIGMIS - Data Base: The Database for Advances in Information Systems*, Vol. 38 No. 1, pp. 60-80, doi: 10.1145/1216218.1216224.

Snail ka Mtuze, S. and Musoni, M. (2023), "An overview of cybercrime law in South Africa", *International Cybersecurity Law Review*, Vol. 4 No. 3, pp. 299-323, doi: 10.1365/s43439-023-00089-8.

SWIFT (2020), "Customer security programme: threat landscape report", available at: https://www.pwc.com/vn/en/services/risk-assurance/cyber-security1/swift-csp.html (accessed 30 March 2026).

Trist, E.L. and Bamforth, K.W. (1951), "Some social and psychological consequences of the longwall method of coal-getting: an examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system", *Human Relations*, Vol. 4 No. 1, pp. 3-38, doi: 10.1177/001872675100400101.

Venkatesh, V., Thong, J.Y. and Xu, X. (2012), "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology", *MIS Quarterly*, Vol. 36, pp. 157-178, doi: 10.2307/41410412.

Verizon (2023), "Data breach investigations report", available at: https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf (accessed 30th March 2026).

Von Solms, B. and Van Niekerk, J. (2013), "From information security to cyber security", *Computers and Security*, Vol. 38, pp. 97-102, doi: 10.1016/j.cose.2013.04.004.

Widiasari, N.K.N. and Thalib, E.F. (2022), "The impact of information technology development on cybercrime rate in Indonesia", *Journal of Digital Law and Policy*, Vol. 1 No. 2, pp. 73-86, doi: 10.58982/jdlp.v1i2.165.

Yar, M. (2013), *Cybercrime and Society*, 2nd ed., Sage Publications, London.

Zulu, M. and Boshoff, R. (2025), "Understanding the cost of economic cybercrime in South Africa: an ambidextrous approach", *South African Journal of Information Management*, Vol. 27 No. 1, a2029, doi: 10.4102/sajim.v27i1.2029.

Further reading

Wall, D.S. (2007), *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge.

Corresponding author

Oluwatoyin Esther Akinbowale can be contacted at: oluwatee01@gmail.com