The Cyber Fraud Threat Landscape

Learnings From Our Recent Cyber Incident Response Engagements in the Financial Services Sector

pwc

Introduction

According to the 2022 PwC Global Economic Crime Survey (GECS), cybercrime was ranked amongst the top 5 types of fraud reported amongst Eastern African respondents. Cyber fraud cases have since become more common as organisations shift to digital services for efficiency, scale, and modernization. Cyber criminals are becoming more sophisticated and perpetrating fewer but more lucrative cyber fraud-attacks.

Financial institutions in particular, are facing more complex cyber-threat vectors as criminals adapt to the institutions' improved control environment and new standards for data protection.

Additionally, with increase in more customer focused service delivery and digital channels e.g., online, self-service portals, mobile banking, internet banking growing exponentially, the uninterrupted availability of critical services becomes a non-negotiable requirement.

In this newsletter, we explore the cyber fraud threat landscape based on insights gleaned from recent digital forensic work done by our experts across Eastern Africa in the financial services sector (banking, microfinance institutions and SACCOs).

We also highlight the implications of cyber fraud threats to institutions, the challenges faced by the sector, and the strategies that institutions can employ to enhance their cyber fraud security measures.

> ....Cybercrime was ranked amongst the top 5 types of fraud reported amongst Eastern African respondents.

How does the cyber fraud threat landscape look like?

Based on our recent digital forensic reviews, we have observed the following patterns of threat vectors exploited by cyber fraud threat actors:

Exploitation of vulnerabilities in customer service and distribution channels

Traditionally, cyber fraud-attacks in the financial sector have targeted core banking systems by gaining unauthorised access to customer accounts through phishing, smishing and collusion. This has been done with a view to compromise the integrity of the systems and thus manipulate account balances and customer information. While these attack vectors targeting the core banking systems still exist, cybercriminals are increasingly targeting alternate banking channels such as, online customer service portals, mobile and internet banking channels and card management systems. These platforms provide access to sensitive information including personal data, account information and transaction histories. They also process a large number of transactions on a daily basis, 24/7. However, some of these channels are implemented hastily to expand and meet client needs and may have less stringent security control measures as compared to the core banking systems, exposing financial institutions to new attack vectors.

One of the vulnerabilities we have observed is lack of comprehensive and consistent client/server validation controls. This may be due to inadequate quality assurance during systems implementation or lack of involvement of key experts e.g., information security or systems fraud risk management specialists during implementation. These vulnerabilities if exploited can allow threat actors to gain unauthorised access to customer details or gain privileged access to internal systems.

Additionally, there has been an increase in the opening of digital accounts which have less stringent Know Your Customer (KYC) requirements as compared to customer accounts opened at the institution's branches. In most cases, KYC information for digital accounts is electronically submitted. This digital process is vulnerable to potential misuse, as users can upload information belonging to individuals other than themselves if proper verification measures are not in place. This contrasts with the traditional method of physical branch visits, where identity verification is typically more secure and reliable.

Consequently, there is an increased risk of cybercriminals creating accounts with fake details and using them to transfer stolen funds.

Exploitation of gaps in systems integration

Systems integration refers to the connection of multiple different IT systems, applications and platforms to ensure they can communicate, send & receive instruction requests, transfer information and operate together efficiently. Service channel systems such as mobile and internet banking rely on third party service providers and integrations which expose financial institutions to additional security risks.

Online service platforms, for example may rely on third party payment gateways and integrations with the core banking system to process transactions. Increase in the number of bank mergers and acquisitions in the also necessitate the consolidation of customer data from the various entities into a single source and integrating systems in some cases. The integrations between systems may be susceptible to attacks if they are not properly designed, configured, secured, and managed.

Additionally, in cases where customer details stored in the alternate banking system database are not properly cross-referenced and synchronized with the accurate data in the core systems at the authentication, validation or authorization stages, the information can be manipulated to link accounts to fraudulent phone numbers and emails or to divulge customer information to unrelated parties.

The ever-rising insider threat

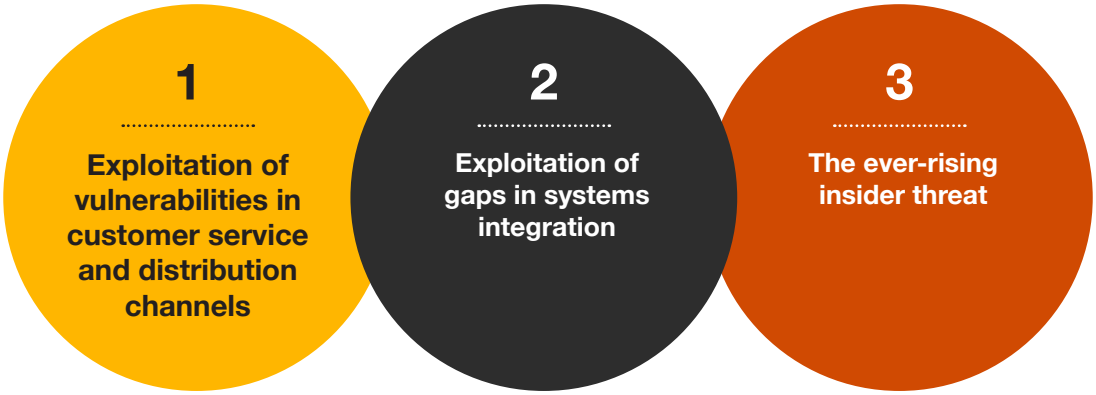
An insider threat encompasses situations where current or former employees, contractors, vendors, or partners misuse their authorised or privileged access system rights or knowledge of an organisation's resources to compromise its networks, systems, and data. These individuals often possess an understanding of the system architecture and exploit weaknesses in Identity and Access Management (IAM) and Privileged Access Management (PAM). They identify and use local accounts with elevated privileges to exploit whitelisted servers with access to sensitive databases, such as the core system's database.

Additionally, we have observed instances where administrator accounts with generic usernames and passwords used by multiple individuals create challenges in tracking and attributing actions.

Social engineering attacks are also a growing concern, as they involve manipulating staff at the institution or customers into divulging sensitive information or providing access to systems. These attacks often involve phishing emails or messages to gain personal information. They may also involve business email compromise (BEC) schemes and invoice spoofing to intercept payments and divert them the attacker's accounts.

In more elaborate schemes, the threat actors collude with non-technical staff requiring them to perform tasks that seem inconsequential or business as usual but are integral to a larger fraudulent operation. The staff are promised a cut of the fraudulent funds in exchange or are threatened. These schemes often involve complex syndicates and can even be on a multinational scale with recruits from both within the institution and outside.

The Cyber Fraud Threat Landscape



Observed consequences of cyber fraud threats to organisations

Cyber fraud incidents may vary in scale from organisation to organisation, however the implications are significant. As in the past, institutions continue to face potential financial loss due to theft of funds, extortion demands, loss of revenue due to downtime and high costs conducting investigations.

In addition, some incidents that we have investigated have resulted in; data breaches and privacy concerns, disruption of critical services , lengthy disciplinary processes and loss of skilled personnel as implicated individuals are dismissed. We have also observed a need for more investment to improve or redo poorly implemented systems and in managing potential negative media coverage. This has been compounded by reputational damage and legal liabilities as well as the involvement of regulators in the case of affected customer accounts.

Common observed hurdles in the management of cyber fraud risks

We have observed some recurring challenges in the management of cyber fraud risks in the region. This is typically due to the dynamic and complex nature of the cyber fraud threat landscape. The following are some of the prevalent challenges we have observed:

- **Lack of automated transaction monitoring:** Organisations struggle to identify suspicious activities due to the lack of robust automated transaction monitoring technology solutions. We find that many institutions either don't have an implemented system or the installed systems are not set up to account for the organisation's unique risk exposures. Some of the automated transaction monitoring solutions are implemented without considering the local context or involvement of fraud risk management teams to tailored detection rules to the specific organizations leading to a lot of false positives.
- **Use of shared accounts/ credentials:** Shared accounts are often used to streamline access to systems, applications, and shared data among team members. However, they do not provide clear accountability for actions performed using the account and can easily be leaked to threat actors.
- **Lack of segregation of duties:** Maintaining proper segregation of duties across an organisation can be difficult even with robust technology, as most organisations have lean human capital resources within the IT department. For example, in some cases roles such as System, Network and Database Administrator roles are held by the same individual or interchanged due to limited delegation matrices.
- **Non-adherence of systems to designed policy/operational manual specifications:** Negligence among stakeholders during system implementation, overreliance on third party vendors and lack of involvement of business teams in various departments may lead to systems that are not properly configured to comply with business product designs, internal policies, allowing systems designated as high-risk to operate outside their intended functional limitations or systems missing critical functionalities that can allow vulnerabilities.
- **Minimal restrictions on unauthorised software:** Lack of control over software installations makes it challenging for organisations to maintain a secure and well-managed IT environment, as they are unable to effectively monitor and restrict the installation of potentially harmful applications. Additionally, some organisations may not have clearly identified permitted and prohibited actions regarding software installations making it difficult to enforce controls.
- **Inadequate reconciliation:** Lack of end-to-end reconciliation to verify the validity and integrity of transactions leaves organisations vulnerable to fraudulent

Consequences of cyber fraud threats

transactions going undetected. In some organisations systems are not properly integrated and automated therefore leading them to resort to manual reconciliations which are time consuming and prone to human error.

- **Inadequate readiness for cyber fraud incident response and forensic investigation:** Without a well-defined incident response plan, organisations struggle to effectively detect and respond to cyber fraud attacks. Additionally, insufficient logging and data retention policies, as well as improper configuration of logging tools, can severely hinder the ability to conduct thorough forensic investigations when cyber fraud incidents do occur. Many organisations fail to retain log data for an adequate period of time, often due to storage constraints or a lack of defined retention requirements.

Other challenges organisations face include: The need to create a balance between security measures and user experience, inadequate cyber fraud detection capabilities, poor or non-existent integration of digital solutions with existing legacy systems, over-reliance on the vendor for system maintenance and lack of accountability, inadequate system controls and configurations, ineffective or absent cyber fraud security measures and system protection and a lack of awareness of emerging cyber fraud trends.

Measures that should be prioritised in mitigating the common cyber fraud breaches

It is essential for organisations to adopt a holistic approach to cyber fraud security that combines technology, training, and proactive incident response strategies to protect their digital assets and sensitive information.

Below are some key measures that we recommend organisations take to safeguard against the common observed cyber fraud threats:

- **Transaction monitoring and fraud management system.** Implementing robust transaction monitoring and fraud management systems can help organisations detect and prevent fraudulent activities in real-time.
- **Privileged user account management and monitoring.** Organisations should implement strict access controls, regularly review, and update user privileges, and monitor privileged user activities for any suspicious behaviour. By closely monitoring privileged and shared accounts, organisations can reduce the risk of insider threats.
- **Proper validation of user/ customer details:** Validating user/customer details is crucial for verifying the identity of individuals accessing systems or services. By ensuring that user information is accurate and legitimate, organisations can prevent unauthorised access, fraud, and data breaches.

- **Ensure implementation of product design policies:** Organisations should ensure all the stakeholders responsible for system configuration, operation, and compliance monitoring understand their roles and are held accountable for adherence to policies.
- **Establish clear software installation policies:** Define and communicate clear policies that specify which software is permitted or prohibited and implement technical controls to limit installations of unauthorised software.
- **Security Information and Event Management (SIEM).** SIEM systems help organisations detect and respond to security incidents by providing real-time analysis of security alerts generated by network hardware and applications. They can also aggregate and correlate log data from multiple systems which is essential for incident response and post-incident forensic analysis.
- **Training and awareness.** Building a strong security culture within an organisation is crucial in mitigating cyber fraud. Regular security awareness training educates employees about cyber fraud threats, best practices, and the importance of following security protocols. A well-informed workforce can act as a line of defence against social engineering attacks and other security risks.
- **Constitution of Board Risk Committee with Cyber Fraud experts:** A technically proficient Board Risk Committee is not just an asset but a necessity in today's digital age, serving as a critical oversight and strategic line of defence against cyber fraud. A board with cyber fraud experts ensures that cybersecurity remains a top priority at the governance level therefore fostering a culture of security awareness throughout the organisation and allocation of sufficient resources to continuously address the constant threats.

Additionally, organisations can implement incident response platforms, and establish a Security Operations Centre (SOC) and Computer Security Incident Response Team (CSIRT).

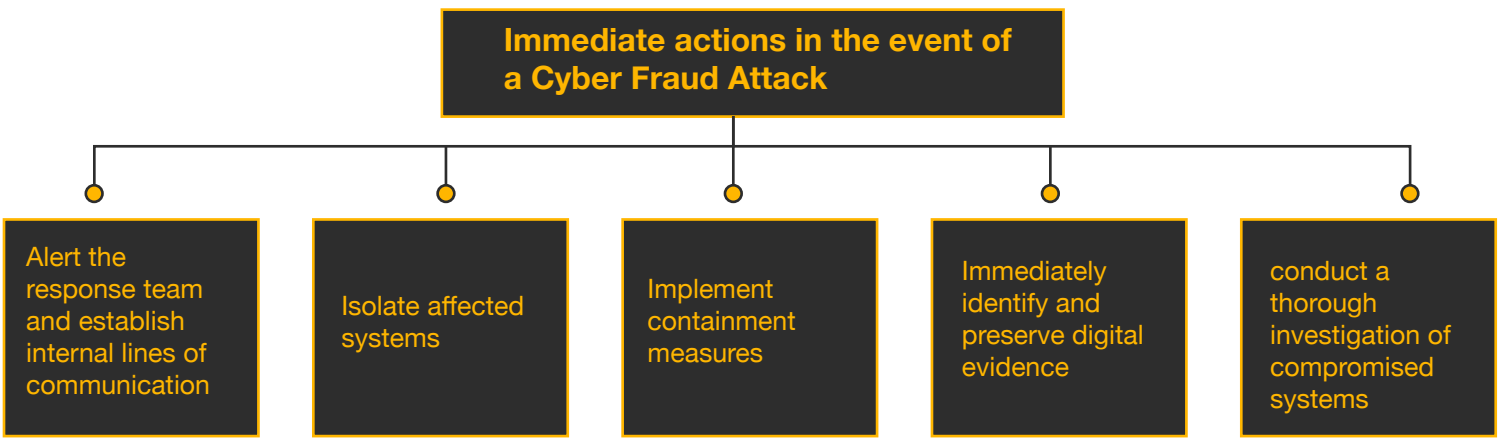
By implementing these measures, organisations can enhance their cyber fraud security resilience, detect, and respond to threats effectively, and mitigate the risks associated with cyber fraud-attacks.

Immediate actions organisations should take in cyber fraud attack response

By taking immediate action, organisations can effectively respond to a cyber fraud -attack, contain the breach, mitigate damage, facilitate recovery, and enhance their cyber fraud security posture. It is essential for organisations to have a well-defined incident response plan in place to guide their actions during a cyber fraud-attack and ensure a coordinated and effective response to security incidents.

Immediate actions organisations can take:

- Alert the response team and establish internal lines of communication: Notify the designated incident response team immediately. Establish clear lines of communication within the organisation to ensure all relevant stakeholders are informed and can coordinate response efforts effectively.
- Isolate affected systems: Quickly isolate the affected systems from the network to prevent further spread of the attack. Disconnecting compromised devices can help contain the breach and limit further damage to other systems and data.
- Implement containment measures: Take proactive steps to contain the cyber fraud-attack by implementing containment measures such as blocking malicious traffic, disabling compromised accounts to prevent the attacker from escalating the breach.
- E-discovery: Organisations should immediately identify and preserve digital evidence



related to the cyber fraud attack in a forensically sound manner to maintain its integrity and admissibility in legal proceedings.

- Digital Forensics (Computer, Cloud, Mobile, Network Forensics and Fraud Analytics): Organisations should conduct a thorough investigation of compromised systems to determine the extent of the breach, identify vulnerabilities exploited by attackers, and understand the attack vectors used. Employing in-depth data analytics enables organisations to assess the full scope of the breach by quantifying the financial losses and identifying any prior attempts of fraudulent activities.

Organisations should also conduct data analysis of system logs, review and update security measures and report the matter to law enforcement to aid in the investigation of the incident.

For further guidance and support, don't hesitate to reach out to us. We are here to provide expert insights and dedicated support tailored to your institution's unique needs. Let's navigate through these challenges together and ensure your business remains resilient and compliant in the face of evolving cyber fraud risk.

Contact us

Andrew Chibuye,
Country Senior Partner,
PwC Zambia,
Tel: +260 (0) 211 334 000
andrew.chibuye@pwc.com

John Kamau,
Associate Director,
Forensics and Lead Financial Crime
PwC East Market Area
Tel: +254 (20) 2855065
john.kamau@pwc.com

Moonga Hamukale,
Associate Director,
Forensics and Financial Crime Advisory,
PwC Zambia
Tel: +260 (211) 334 000
moonga.hamukale@pwc.com