Forensics Digest

December 2025

The Cyber Fraud Threat Landscape: A focus on Third-Party Risk

According to the PwC 28th Annual Global CEO Survey, 24% of the CEOs identified cyber risks as one of the biggest threats their organizations are highly and extremely exposed to in the year ahead, ranking it third overall.

Introduction

The SolarWinds attack, which compromised over 18,000 organizations through a single trusted software update, stands as a stark reminder that in today's interconnected digital ecosystem, your cybersecurity is only as strong as your weakest vendor. What began as a routine software patch became one of history's most sophisticated third-party attacks.

This sobering reality has resonance across Eastern Africa's rapidly digitalizing financial sector, where institutions are increasingly discovering that their greatest cyber vulnerabilities no longer reside within their own four walls. According to the PwC 28th Annual Global CEO Survey, 24% of the CEOs identified cyber risks as one of the biggest threats their organizations are highly and extremely exposed to in the year ahead, ranking it third overall. In their push for digital transformation, financial institutions have built extensive dependence on vendors, cloud service providers and fintech partners. This concentrated reliance has reshaped the threat landscape and heightened their exposure to cyber and insider risks.

Based on recent digital forensic investigations we have conducted across Eastern Africa's financial services sector, we have observed a pattern that should concern every industry leader: third-party vendors are increasingly becoming the preferred attack vector for sophisticated cybercriminals. These external partners, armed with privileged access to critical systems and sensitive data, represent both the greatest opportunity for institutional growth and the most significant threat to institutional survival. The challenge is no longer simply about building higher walls around your own systems, it's also about ensuring that every bridge you build to the outside world is fortified against those who would exploit your trust.

Let's take a deep dive into what third party cyber risk looks like for your organization.

Organisations must treat third-party access as a privilege, not a default. Vendors should never operate with unrestricted or unmonitored access. All activity must be scoped, time-bound and logged, with clear accountability and involvement from internal IT and cybersecurity teams.

What is third-party risk?

Third party risk encompasses the multifaceted threats and vulnerabilities that arise when institutions engage external vendors, service providers or partners in their operations. We outline the following third-party risks that we have observed within the region.

Unmonitored vendor access

An often-overlooked cyber risk lies not in third-party vendors being compromised by external threats, but in the vendors, themselves becoming a direct threat to the organisations they serve. In some cases, vendors are granted extensive, persistent and largely unsupervised access to internal systems, access that rivals or even surpasses that of internal IT teams.

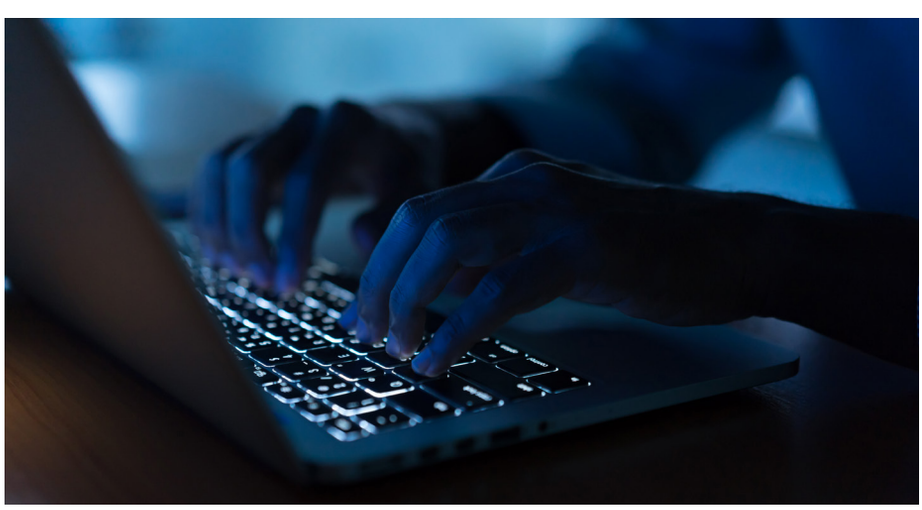
In other situations, business users sometimes bypass the internal IT team altogether by contracting vendors directly and granting remote access to the vendor through unsecured channels. This creates a shadow operational layer where critical system activities occur outside formal governance structures.

Such arrangements assume the vendor will always act in good faith. However, this is a significant gamble. When a third party has full visibility and control over the IT environment, the organisation effectively relinquishes a portion of its risk to an external entity. In a recent engagement, we observed the finance operations team providing vendors with rights to remotely control their computers via unlicensed remote access tools when seeking support services on the vendor's system, without IT oversight. The access was unsupervised, exposing the organization to significant risks of unauthorized system activity and potential data manipulation.

To manage this risk, organisations must treat third-party access as a privilege, not a default. Vendors should never operate with unrestricted or unmonitored access. All activity must be scoped, time-bound and logged, with clear accountability and involvement from internal IT and cybersecurity teams. Where this oversight is missing, the vendor is not just a partner, they become a potential insider threat operating outside the organisation's line of sight.

Contractual risk

A well-structured contract serves as a frontline defence in today's dynamic digital threat landscape. Contractual risks emerge when agreements with third parties such as vendors, service providers and partners lack clear terms that speak to key security aspects. These aspects include but are not limited to data protection, data ownership and control, breach notification timelines, subcontractor and supply chain obligations, audit and monitoring rights, termination and data deletion clauses, liability and indemnity clauses, service level agreements (SLAs) among other aspects. When these clauses are omitted or their inclusion is vague, threat actors and cybercriminals gain exploitable gaps, allowing them to breach systems and manipulate data with little to no accountability.



Contracts must proactively anticipate and explicitly define the secure responsibilities of all parties, ensuring alignment and accountability across high-risk digital environments.

One of the critical consequences of third-party underperformance is the creation of operational blind spots particularly in fraud detection. If a vendor responsible for monitoring or alerting systems fails to function optimally, suspicious activity can go unnoticed.

When third parties manage sensitive data or transaction workflows, any breakdown in performance can create exploitable gaps that fraudsters can take advantage of often without immediate detection.

In a recent engagement, we encountered a case involving a financial institution that relied on a third-party software vendor to provide digital financial services to its customers. However, the agreement between the two parties lacked specific clauses on data sharing. Most notably, it did not obligate the vendor to provide the detailed transactions level data or associated system logs. As a result, when suspicious activity was suspected on the vendor's platform, the institution was unable to access sufficient data to trace its origin and nature.

In an era of increasingly interconnected digital ecosystems, vague contractual language doesn't merely introduce legal ambiguity – it opens the door to real and measurable cyber threats. Contracts must proactively anticipate and explicitly define the secure responsibilities of all parties, ensuring alignment and accountability across high-risk digital environments. Additionally, organizations should not only ensure that contracts are clear and comprehensive but also engage qualified legal counsel and cybersecurity experts during the contracting stage. These professionals can help identify potential vulnerabilities, craft precise clauses, and align contractual obligations with regulatory and operational requirements.

Performance risk

Third-party performance risk arises when external vendors or service providers fail to meet agreed-upon service levels, directly impacting an organization's ability to deliver critical services, maintain operational continuity, or detect and respond to fraud in a timely manner. This can include delays in software updates, system outages, or inadequate support from cloud or cybersecurity vendors. Such underperformance can degrade user experience, disrupt internal processes, and increase operational vulnerability.

One of the critical consequences of third-party underperformance is the creation of operational blind spots particularly in fraud detection. If a vendor responsible for monitoring or alerting systems fails to function optimally, suspicious activity can go unnoticed. Similarly, slow response times, missed alerts, or poor data handling can hinder an organization's ability to detect and investigate anomalies, escalating the risk of financial loss or reputational damage before any intervention can be made.

Beyond oversight failures, underperforming vendors can directly enable fraud by weakening key control environments. For example, delays in applying cybersecurity patches may expose systems to exploitation, or poor identity verification processes may allow unauthorized access. When third parties manage sensitive data or transaction workflows, any breakdown in performance can create exploitable gaps that fraudsters can take advantage of often without immediate detection. An example is an investigation we conducted in one of the top-tier banks in East Africa that relied on a third-party for its mobile banking services through its Unstructured Supplementary Service Data ("USSD") platform. Whereas the contract between the bank and the third-party required the third-party to proactively identify defects in the services, and advise the bank on a timely manner, we noted an incident perpetrated by a former employee of the third-party which went undetected by the vendor. The incident was later uncovered by the bank's internal reconciliation team who noted multiple bank-to-customer transactions with no origination from the bank's core banking system.

To mitigate third-party performance risk, organizations should implement a robust vendor risk management framework that includes continuous monitoring, clear contractual obligations, and contingency planning. This begins with thorough due diligence during vendor selection, ensuring providers have a proven track record and the capacity to meet performance expectations. Service level agreements should be detailed and enforceable, outlining specific metrics for uptime, response times, and fraud detection capabilities. Regular audits and performance reviews help identify issues early, while real-time monitoring tools can detect anomalies in vendor systems

To mitigate third-party insider threats, organizations should enforce robust access controls, ensure timely deactivation of credentials after contract completion, conduct continuous monitoring of third-party activities, and evaluate vendors' internal security practices.

that may signal underperformance. Additionally, organizations should maintain internal capabilities to ensure continuity in case of failure and establish incident response protocols that include vendor coordination to swiftly address any disruptions or vulnerabilities.

Insider threats from the third party

Third-party insider threats arise when external individuals or entities such as contractors, vendors, consultants, or outsourced service providers who are granted access to a company's systems, data, or infrastructure. These actors, while not employees, can pose significant risks if their access is misused, compromised, or left unchecked.

Such threats may stem from malicious intent, for example third parties being compromised by external attackers, using stolen credentials to infiltrate the host organization. In a recent engagement, we encountered a scenario where a third-party threat actor diverted funds by abusing privilege system access, exploiting system integration vulnerabilities to intercept and send spoofed emails with manipulated payment details.

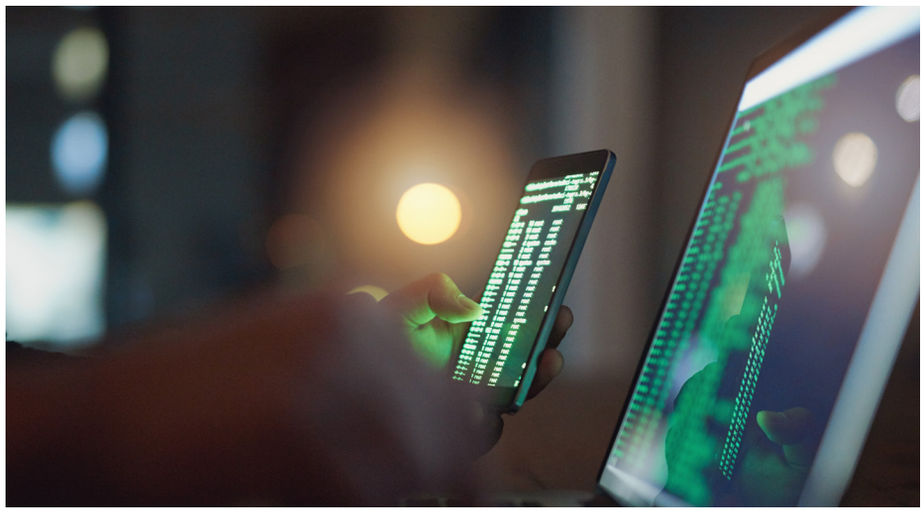
Additionally, we observed a case where a former employee whose access to the Application Programming Interface (API) wallet credentials was not promptly revoked after departure, and he utilised the access to push unauthorized multiple disbursements to several mobile wallets.

The impact of third-party insider threats includes financial fraud, for instance when payment instructions are manipulated during the procurement process, data breaches resulting from unauthorized data access or transfer, intellectual property loss, and reputational damage when sensitive information is leaked. Misuse of privileged access, especially when granted to external IT or support personnel, further compounds the risk.

To mitigate third-party insider threats, organizations should enforce robust access controls, ensure timely deactivation of credentials after contract completion, conduct continuous monitoring of third-party activities, and evaluate vendors' internal security practices. Incorporating behavioral analytics and requiring security awareness training for external partners can also strengthen defences against these often-overlooked vulnerabilities.

Reputational risk

Reputational risk is one of the most intangible yet consequential outcomes of third-party involvement in the cyber fraud landscape. In today's interconnected financial ecosystem, institutions rely on third parties for critical business processes. However, in instances where errors or manipulations occur at the third party, the primary institution may be perceived as the source of compromise, regardless of where it occurred. For example, if a customer's transaction is diverted



A single breach at a vendor can expose sensitive customer or operational data, disrupt services, and severely damage an organization's reputation and regulatory standing.

to an unintended recipient due to irregularities in the processing chain, the affected customer will typically hold their bank accountable for the loss, even when the deviation occurred within an external vendor's system beyond the bank's immediate oversight.

In one case we examined, a malicious insider at a third-party vendor exploited vulnerabilities in the payment instruction system to redirect funds to an unauthorized account. Although the breach occurred entirely within the vendor's infrastructure, the bank remained unaware of the compromise and processed the fraudulent transaction through standard protocols. However, the bank's infrastructure still came under public scrutiny, with a primary focus on the financial institution's role in the incident.

The reputational impact is often amplified by limited transparency into third party processes and the public's expectation that financial institutions maintain end to end control. It is also compounded by the speed and scale of information dissemination in the digital age. Social media, online reviews, and news cycles can amplify incidents rapidly, often before the facts are fully understood. This highlights the need for enhanced due diligence and clearly defined responsibilities across the transaction chain to mitigate reputational fallout from third party actions.

Data breaches

Organizations increasingly rely on third-party vendors for services such as cloud storage, IT support, and payment processing. While this outsourcing enhances efficiency, it also introduces significant cyber risk, particularly through data breaches at third-party providers. A single breach at a vendor can expose sensitive customer or operational data, disrupt services, and severely damage an organization's reputation and regulatory standing.

In Eastern Africa, the regulatory frameworks like Kenya's Data Protection Act and Uganda's Data Protection and Privacy Act place accountability on data controllers even when the breach occurs at a third party. Recent incidents across financial and telecom sectors have shown how such breaches can lead to legal penalties, erosion of customer trust, and operational downtime.

To mitigate this risk, organizations must adopt a robust third-party risk management strategy. This includes conducting due diligence before onboarding vendors, enforcing data handling and cybersecurity standards through contracts, and continuously monitoring vendor compliance. Additionally, incident response plans should account for third-party breaches, ensuring timely containment and communication. In this interconnected ecosystem, protecting data means ensuring partners protect it too.

Services Provided by the PwC Forensics Team:

- Conducting Fraud Risk Assessments
- Carrying out Enhanced Due Diligence
- Providing Investigative Support
- Providing Litigation Support

Conclusion

As the cyber fraud landscape evolves, third-party risk remains one of the most complex and consequential challenges facing financial institutions in Eastern Africa. From concentration and performance failures to insider threats, data breaches, and reputational damages, the examples highlighted in this newsletter underscore the need for a proactive and structured approach to third-party risk management. At PwC, our Cyber and Digital Forensics team supports institutions in navigating these risks through a suite of tailored services.

Conducting Fraud Risk Assessments:

We identify control gaps in third-party relationships to proactively mitigate potential risks. This includes analyzing concentration risks, where vendors may have excessive access to systems, and evaluating contractual agreements for security-related clauses. We help organizations treat third-party access as a privilege, ensuring all activities are scoped, time-bound, and logged with clear accountability.

Carrying out Enhanced Due Diligence:

We thoroughly investigate vendors and partners to ensure their reliability and compliance.

This process involves comprehensive background checks, financial analysis, and evaluation of operational capabilities.

We also assist with contract reviews to identify potential vulnerabilities, ensuring proper risk allocation and inclusion of essential security clauses such as data protection, breach notification, and audit rights.

Providing Investigative Support:

We offer expert assistance in cases of suspected fraud or data compromise. Our team employs advanced digital forensics techniques and cyber investigation methodologies to uncover evidence and provide actionable insights. We help organizations address performance risks that may create operational blind spots or enable fraud through weakened control environments. Additionally, we assist in identifying and mitigating insider threats from third parties.

Providing Litigation Support:

We offer expert guidance and evidence in legal disputes related to third-party issues. Our team can assist with case strategy, evidence collection and analysis, and expert witness testimony. We leverage our industry expertise and legal insights to support your position effectively, particularly in cases involving data breaches, reputational damage, or contractual disputes arising from third-party relationships.

Our multidisciplinary approach blends digital forensics, cyber investigations, legal insights, and industry expertise to help clients anticipate, detect, and respond to third-party cyber fraud threats with confidence. We aim to strengthen your organization's third-party risk management practices, ensuring a more secure and resilient business environment in the face of evolving cyber threats.

Contact us

Andrew Chibuye
Country Senior Partner
andrew.chibuye@pwc.com

John Kamau
Partner, Forensics Services
john.kamau@pwc.com

Lyndon Lane-Poole
Partner, Consulting & Risk Services
lyndon.l.lane-poole@pwc.com

Moonga Hamukale
Associate Director, Deals
moonga.hamukale@pwc.com

Josephat Mwanzia
Manager, Forensic Services
josephat.mwanzia@pwc.com

Isaac Gachigua
Manager, Forensics Services
isaac.gachigua@pwc.com