pwc

Strengthening cybersecurity in Rwanda's SACCOs amid digital transformation

In pursuit of Rwanda's vision for inclusive economic growth and financial empowerment, the country's financial institutions are rapidly digitalising their service delivery models. This digital transformation, driven by innovative technologies, seeks to extend financial access to underserved communities, increase operational efficiency, and contribute to the achievement of Rwanda's sustainable development goals.

Savings and credit cooperatives (SACCOs) are a cornerstone of Rwanda's financial ecosystem, playing a pivotal role in promoting grassroots financial inclusion and driving local economic empowerment. The recent automation of systems across all 416 Umurenge SACCOs has significantly transformed the subsector by accelerating the adoption of digital service channels. These include mobile banking, digital wallets, front office services (FOSA) such as deposits, withdrawals, and loans, and automated transaction platforms.

While this digital transformation brings numerous advantages, such as enhanced service delivery, expanded outreach, and improved operational efficiency, it also introduces increasing cybersecurity risks. These risks include potential financial losses, data breaches, fraud and account takeover, system vulnerabilities, operational disruptions (such as ransomware), regulatory penalties, reputational damage, and AI driven threats (including deepfakes, synthetic identities, and advanced social engineering). If not adequately managed, such risks can undermine the essential principles of confidentiality, integrity, and availability of data, which are fundamental to maintaining trust and ensuring the sustainability of Rwanda's financial sector.

Why SACCOs are prime cybercriminal targets

Several factors contribute to the elevated cybersecurity risk profile of SACCOs. A primary concern is their reliance on supply-chain dependencies, as SACCOs frequently integrate with various external third-party platforms including core banking vendors, mobile money services, payment gateways, managed service providers, and system integrators. These multiple interconnected systems create numerous points of vulnerability that attackers can exploit. In addition, SACCOs operate under a trust-based membership model, heavily depending on the confidence and loyalty of their members and communities. Any breach that compromises this trust can lead to significant declines in member confidence, which in turn threatens the very survival of these institutions.

Furthermore, SACCOs safeguard high-value data, such as members' savings, loan records, and transaction histories, which are attractive targets for cybercriminals interested in financial fraud or identity theft. The regulatory and financial stakes are also substantial; cyberattacks can lead to hefty regulatory penalties, direct financial losses, and reputational damage. Compounding these risks is the perceived security maturity of SACCOs, which often operate with limited budgets, small IT teams, outdated systems, limited 24/7 monitoring, and slower patch management compared to larger financial institutions.
This perception of weaker cybersecurity infrastructure positions SACCOs as easier and more vulnerable targets for cyberattacks.

The growing cyber threat landscape in Africa—and Rwanda's SACCOs

3 billion

in cybercrime losses between 2019 and 2025.

The rapid expansion of digital financial services across Africa has significantly enhanced financial inclusion and economic growth. However, this progress has been accompanied by a sharp rise in cybercrime. INTERPOL's Africa Cyberthreat Assessment Report 2025 projects that Africa will incur over USD 3 billion in cybercrime losses between 2019 and 2025, with the financial sector among the hardest hit, followed by healthcare, energy and government sectors.

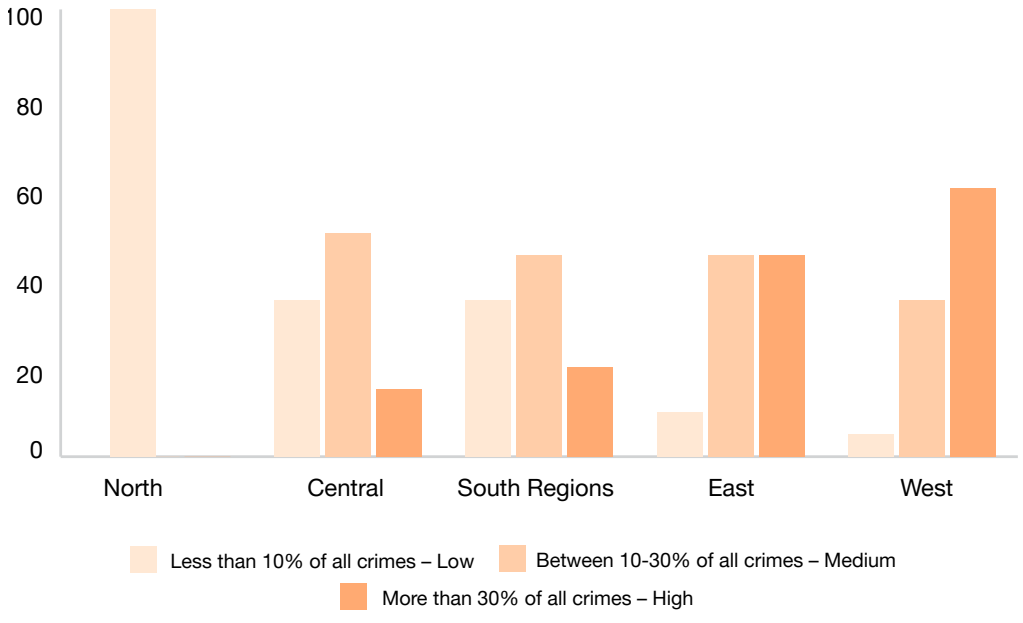
30%

of all reported criminal activity, posing critical risks to Rwanda's SACCOs.

In Western and Eastern Africa, including Rwanda, cyber-dependent and cyber-enabled crimes account for more than 30% of all reported criminal activity, posing critical risks to Rwanda's SACCOs.

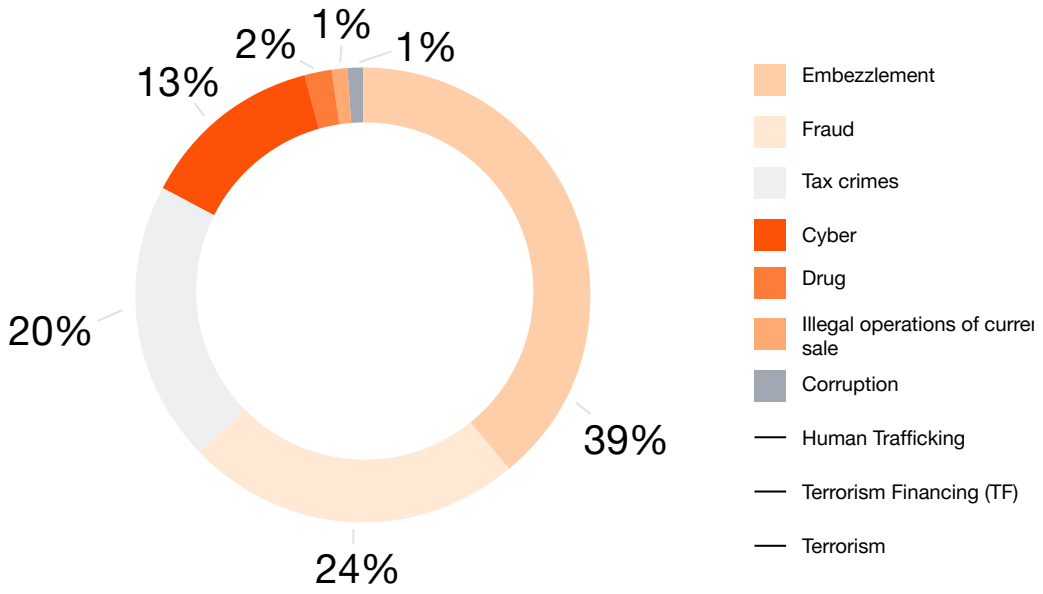
These institutions, essential for grassroots financial inclusion, face threats that extend beyond financial loss, including impact on national economic stability and public trust.

Figure 1: Perceived cybercrime risk levels across African subregions as reported by INTERPOL Africa member countries in the 2025 Survey



The 2024 National Money Laundering and Terrorist Financing Risk Assessment reports that over the past five years, 90 cyber-crime cases were detected, accounting for 13% of total crime proceeds. Of these cases, 66 were prosecuted, resulting in 39 convictions involving 62 suspects. The rise in internet access and digital financial services has enabled criminals to exploit technologies such as hacking, phishing, and malware to unlawfully access financial systems and manipulate or steal funds. These findings highlight both the growing threat of cyber fraud and critical gaps in Rwanda's ability to detect, prevent, and respond to cybercrime within its digital financial services sector.

Fig. 2 Percentage share of predicate offences with large amount of money.



Highlighting the urgency of the issue, PwC's Digital Trust Insights Survey for East Africa reveals that 74% of businesses in the region now prioritise cybersecurity. This represents a growing recognition that cybersecurity is no longer a technical concern limited to IT teams but a fundamental business imperative. For SACCOs in Rwanda, implementing robust cyber resilience is essential to preserving organisational resilience, protecting member assets, maintaining stakeholder trust, and supporting sustainable growth within the country's rapidly evolving digital economy.

Strategic imperatives for SACCO cybersecurity

To navigate the evolving cyber threat landscape, Rwanda's SACCOs must adopt robust, multi-layered cybersecurity strategies that align with both national priorities and international best practices. This begins with adherence to national frameworks such as directives from the National Bank of Rwanda, the National Cybersecurity Authority, Data Protection Law, the National AI Policy, and the Financial Sector Development Strategy. Strong governance and leadership are essential, requiring SACCOs to establish comprehensive cybersecurity and data privacy policies, embed privacy by design principles, and form dedicated teams responsible for regular risk assessments and vulnerability remediation, and manage cyber insurance aligned to their risk appetite. Embracing zero trust security principles by continuously authenticating and authorizing all users, devices, and applications—regardless of their network location—is critical to preventing unauthorised access.

Furthermore, SACCOs should foster a culture of cybersecurity awareness through ongoing training and phishing simulations to reduce human error, while adopting holistic frameworks like NIST Cybersecurity Framework (CSF), ISO/IEC 27001, ISO/IEC 42001, or Center for Internet Security Controls (CIS) for effective information security management. Investing in advanced security technologies such as endpoint protection, firewalls, intrusion detection/prevention systems, network segmentation, encryption, and multi-factor authentication will help minimise risk exposure. Continuous risk management through real-time monitoring, vulnerability assessments, penetration testing, and strict user access controls following the principle of least privilege are vital. Incident preparedness requires clear, tested response and disaster recovery plans supported by secure, encrypted data backups. Data privacy must be prioritised, ensuring the confidentiality and integrity of member information, while stringent oversight of third-party partners is necessary to mitigate supply chain risks. Lastly, SACCOs should engage collaboratively with regulators and industry bodies like the Rwanda Information Society Authority (RISA), The CyberHub and the National Bank of Rwanda for threat intelligence sharing, capacity building, and coordinated cybersecurity defence.

By integrating these strategic imperatives into their operational frameworks, SACCOs in Rwanda can strengthen their cybersecurity posture, safeguard member assets, maintain regulatory compliance, and foster sustainable financial inclusion through secure digital innovation

Conclusion

Rwanda's SACCOs stand at the forefront of the country's financial inclusion agenda, empowered by digital innovation to extend critical financial services. However, the promise of digital transformation can only be fully realised if cybersecurity is embedded as a fundamental business priority. Protecting the security of member data, maintaining regulatory compliance, and ensuring operational resilience require a unified commitment from the boardroom to frontline staff.

Only by adopting comprehensive cybersecurity measures can SACCOs safeguard the trust and financial stability of the communities they serve. Ultimately, embedding cybersecurity as an intrinsic element of their operations will reinforce Rwanda's vision for a resilient, inclusive, and prosperous digital financial ecosystem.

Cybersecurity in SACCOs is not a luxury in the digital age; it's an indispensable necessity.

Authors

Anthony Njeeh – Associate Director

PwC Rwanda (Government and Public Sector)
Email: anthony.k.njeeh@pwc.com

Alex Mihigo – Senior Associate

PwC Rwanda, C&RS
Email: alex.mihigo@pwc.com

Thank you