Effective information security leadership is key

In Uganda's rapidly digitising economy, information security is no longer a back-office function delegated solely to IT teams. It has become a strategic leadership imperative. In an era defined by escalating data breaches, privacy violations and sophisticated cybercrime, effective leadership is the cornerstone of a resilient and trusted information security framework.

The financial impact alone is sobering. According to the 2024 Annual Police Crime Report, Ugandans and businesses lost more than $272m (Shs958b) to cyber fraud and bank-related scams in 2024.

Against this backdrop, leadership must rise above operational oversight and embrace information security as a core governance responsibility.

A robust information security foundation must be deliberately constructed. This includes adopting internationally recognised standards and best practices such as ISO 27001, the NIST Cybersecurity Framework and data protection principles aligned with Uganda's Data Protection and Privacy Act. These frameworks are not symbolic certifications. They are structured mechanisms for identifying risks, protecting critical assets, detecting threats, responding effectively and recovering swiftly.

The Cyber Risk Management Directive issued by the Bank of Uganda in 2024 marked a decisive shift in accountability. Cybersecurity oversight is no longer an implied responsibility. It is explicitly assigned to boards of supervised financial institutions.

This regulatory development places leadership at the centre of institutional cyber resilience. Boards are expected to, among other things; endorse comprehensive cybersecurity risk and resilience action plans, prioritise governance structures, awareness programmes and recovery maturity, mandate quarterly cybersecurity and data privacy reporting and integrate cybersecurity key performance indicators into executive performance scorecards

> Recovery from a destructive cyber incident is not improvised. It is engineered in advance.

Catherine Bwire
Information security

Effective information security leadership requires a risk-based mindset. Leaders must understand the organisation's risk exposure, the value of its information assets and the potential financial, reputational and regulatory consequences of a breach.

Risk appetite and tolerance are shaped at senior management level. Decisions on whether to invest in preventative controls, advanced monitoring tools, cyber insurance or large-scale recovery infrastructure are strategic financial choices. They directly determine the scale of damage when an incident occurs.

Leadership that underestimates cyber risk does not reduce cost. It defers it, often at a significantly higher price.

Representation of information security at board level is no longer optional. The modern Chief Information Security Officer serves as a strategic advisor, translating complex technical risks into business language that resonates in the boardroom.

An empowered CISO facilitates a structured bottom-up flow of information on emerging threats, vulnerabilities and incident trends. At the same time, they ensure top-down communication of strategic decisions to operational teams. This alignment strengthens institutional coherence and accountability.

More importantly, the CISO provides data-driven insights linking security posture to brand reputation, regulatory exposure, investor confidence and business continuity. In doing so, cybersecurity becomes integrated into enterprise risk management rather than isolated as a technical silo.

Leadership support is critical in mapping and understanding technological assets that underpin core operations. Many organizations operate with fragmented visibility of their infrastructure, third-party dependencies and data flows.

True resilience demands investment in; secure system architecture and network segmentation, continuous threat monitoring and intelligence capabilities, robust backup strategies with offline and immutable backups, large-scale recovery and rebuild capabilities, regular threat-led penetration testing and scenario simulations. Recovery from a destructive cyber incident is not improvised. It is engineered in advance.

In Uganda's competitive financial and corporate landscape, institutions that demonstrate mature information security governance will command greater trust from customers, investors and regulators.

Ms Catherine Bwire, Head, Information Security & Data Privacy, Ecobank Uganda