Why physical security still matters in a digital age

The recent theft of laptops from the Bank of Uganda is a sobering reminder that even in an era of rapid digital transformation, physical security remains a foundational pillar of institutional integrity. As organisations race to adopt Artificial Intelligence, strengthen data governance, and migrate operations to the cloud, a critical vulnerability is being overlooked: information systems are only as secure as the physical environments that house them.

International standards make this explicit. ISO/IEC 27001:2022, the globally recognised benchmark for information security management, includes physical controls among its 93 required controls. Its companion standard, ISO/IEC 27002, provides detailed guidance on implementing safeguards that prevent unauthorised physical access, damage, or interference with information and information processing facilities. These are not optional considerations. They are compliance obligations.

Physical security extends well beyond guards and locked doors. It encompasses controlled access systems, surveillance mechanisms, secure storage policies, visitor management protocols, and clear desk and clear screen practices. The singular objective is to ensure sensitive information assets, whether digital or physical, are protected from theft, loss, or compromise.

> The integrity of our systems, and the trust of the public, depends on getting the fundamentals right.
>
> **Paul Kwiringira**
> **Cyber security**

The stakes become clearer when applied to an institution like a central bank. Such organisations hold both personal and sensitive data belonging to customers, employees, and the State itself, stored on servers, computers, and portable devices. A stolen laptop, if unencrypted or improperly secured, can expose this data entirely. Under data protection frameworks, organisations are legally obligated to ensure the confidentiality and integrity of such information. Physical negligence translates directly into legal liability, reputational damage, and erosion of public trust. The Bank of Uganda incident raises important questions that go beyond the theft itself. How were devices containing potentially sensitive information accessed and removed? Were adequate access controls in place? Were asset management protocols, including device tracking and encryption, effectively implemented?

What, then, should organisations do?

Begin with a physical security risk assessment aligned with ISO frameworks. Identify where vulnerabilities exist, from server rooms to open-plan offices, and address them systematically. Integrate physical and information security policies into a single, unified approach rather than treating them as separate functions. Invest in staff awareness, because even the most sophisticated systems can be undermined by human oversight. Finally, establish incident response mechanisms that treat physical breaches with the same urgency as cyber-attacks.

The lesson here is that security is holistic. As organisations invest in firewalls, encryption, and endpoint protection, they must apply equal rigour to the physical environment: locked doors, biometric entry controls, privileged access to sensitive records, and enforced clean desk policies. One without the other leaves institutions exposed.

The integrity of our systems, and the trust of the public, depends on getting the fundamentals right.

Mr Paul Kwiringira, associate at KTA Advocates.