Kingsgate Advisors Institute

Commentary

Cybersecurity in an Evolving Digital Economy: Essential Insights You Need to Know

Funmilayo Akinti
Founder, Saberlight TechSecure Systems

In today's increasingly digital world, cybersecurity has become a critical issue that extends far beyond the realm of technology. It is now a matter of national security, economic stability, public trust, and investor confidence. The rapid pace of digital transformation, fueled by innovations such as mobile money and e-government platforms, has created new vulnerabilities that require immediate attention.

While the benefits of digital connectivity are undeniable, the corresponding investment in cybersecurity is lagging behind. Every day brings a new wave of applications and services designed to simplify life. However, this simplicity often comes at the cost of increased risk. Security is frequently treated as an afterthought rather than being embedded in the development process from the outset. This delay has created a dangerous imbalance. As digital infrastructure grows, so too does the opportunity for exploitation.

Globally, we are witnessing a sharp increase in threats, including ransomware and deepfake-driven attacks. The ease with which bad actors can now launch sophisticated cyberattacks, thanks to tools like artificial intelligence, has led to significant financial losses and reputational damage for both public and private institutions. The emergence of "ransomware as a service" underscores the commodification of cybercrime, enabling even non-technical individuals to launch damaging attacks. In regions such as the Global South, where digital adoption is growing rapidly, new risks are emerging. Practices like SIM swap fraud, which exploits mobile identity verification systems, and API vulnerabilities, which compromise multiple services through a single point of failure, are becoming alarmingly common. Databases housing sensitive personal information, such as national ID systems or banking records, are particularly vulnerable and often lack adequate safeguards. A single breach can have cascading effects across numerous platforms and institutions.

Additionally, social engineering and phishing attacks have become more effective as personal data is increasingly scattered across various online platforms. People interact with numerous vendors and services daily, often unaware of how exposed their information is. This fragmented exposure makes it easier for attackers to craft convincing scams. Small and medium-sized enterprises (SMEs), in particular, face a daunting challenge. With limited budgets and often just a staff handling both IT and cybersecurity functions, these businesses are especially vulnerable. Many assume that cyberattacks only target large corporations, but the truth is that smaller organisations are often seen as easier targets.

The question is, how do we mitigate against these risks? Simple steps can make a significant difference. Embedding security practices into onboarding policies, utilising password managers, implementing two-factor authentication, and conducting regular security awareness training can all help protect against threats. Data should be backed up frequently, and systems updated promptly. Even posting physical reminders, such as charts for backup schedules or update logs, can improve adherence to best practices.

Cybersecurity is not merely a technical issue but a cultural one. Digital literacy forms the bedrock of resilience. Employees must understand not only the tools they use but the risks associated with them. Many organisations invest heavily in infrastructure, only to see their defences compromised by a single act of carelessness, such as tailgating into a secure area or clicking on a suspicious link. People are often the weakest link in the security chain.

Unfortunately, digital literacy is not evenly distributed. Most training occurs once a year, if at all, and is often limited to IT departments. To be effective, awareness must be consistent and universal, spanning from interns to executives. Language is another barrier. Many awareness campaigns fail to reach older or rural populations due to the lack of materials in local dialects. Additionally, many assume they are immune to cyber threats, adopting a false sense of security that makes them even more vulnerable.

Cyberattacks carry tangible economic costs. Reputational damage, financial loss, and diminished public trust are common outcomes. Businesses that fall victim may struggle to recover. Customers become wary, investors pull back, and competitors seize opportunities. In some cases, the aftermath extends to critical infrastructure. Disrupted services, such as healthcare or banking, can have life-threatening consequences.

Strong cybersecurity policies are essential, especially in emerging economies. Unfortunately, most existing frameworks are reactive. Policies are often enacted only after an incident has occurred, and few mechanisms exist for enforcement or evaluation. Effective policies should be tied to incentives. For example, just as businesses must present tax clearance certificates or CAC registration to access government funding, proof of cybersecurity training or compliance should become a requirement.

A national baseline standard should also be introduced. A minimum-security posture should be mandated for all service providers and infrastructure operators. Before apps are launched or cloud services offered, they should be audited by an independent body to ensure they meet security requirements.

Furthermore, awareness efforts must be decentralised and localised. Campaigns should be delivered in indigenous languages and tailored to the local cultural context. Finally, a national cybersecurity body should operate around the clock, managing risk, coordinating responses, and ensuring consistent enforcement.

In conclusion, cybersecurity is not optional. It underpins everything from economic growth to public safety. As technology becomes increasingly integrated into daily life, securing the digital domain is not just prudent. It is imperative.

The views expressed in this article are those of the author(s) and do not necessarily reflect the views of Kingsgate Advisors Institute.

About the Author

Funmilayo Akinti is a seasoned IT and business operations leader with over a decade of experience driving strategic growth across the finance, telecom, and energy sectors. As the founder of Saberlight TechSecure Systems, she's passionate about cybersecurity, risk analysis, and aligning technology with business outcomes.

About Kingsgate Advisors Institute

Kingsgate Advisors Institute is a nonprofit, nonpartisan research organization that develops innovative solutions to improve policy and decision-making and empower economies at the local, national and global levels to unlock their full potential.

Contact us:

If you have questions and comments about this article and for more inquiry about our research at Kingsgate, you can reach us via this email info@kingsgateinstitute.org or visit our website at www.kingsgateinstitute.org

Kingsgate
Advisors
Institute

CONNECT WITH US:

kingsgate_advisors_institute

Kingsgate Advisors Institute

Kingsgate Advisors Institute

www.kingsgateinstitute.org

Kingsgate
Advisors
Institute