



INAUGURAL NATIONAL CYBERSECURITY CONFERENCE

Kampala, Uganda | 11 August 2026

KEYNOTE ADDRESS BY THE GOVERNOR, BANK OF UGANDA

“Trust by Design: Building a Cyber-Resilient Digital Economy for Uganda”

Theme: Securing Uganda's Digital Future — Collaboration, Resilience and Trust

Honourable Minister of ICT and National Guidance;
Honourable Ministers and Government Officials;
The Chairperson, Executive Director, and Members of the Uganda Communications Commission, and the leadership of UgCERT;
Heads and representatives of our security and other national institutions;
Distinguished development partners;
Leaders from the financial sector, telecommunications and technology industries, academia and the private sector;
Ladies and Gentlemen.

Good morning.

It is a privilege to join you at this inaugural National Cybersecurity Conference. On behalf of the Bank of Uganda, let me commend the Uganda Communications Commission, UgCERT, and every partner who made this gathering possible. That this room holds regulators and security agencies, bankers and telecom operators, technologists and academics, development partners and public servants, is itself the argument I have come to make: cybersecurity is no longer the responsibility of one institution. It is a national capability.

Hon. Nyombi Thembo, with your indulgence: the keynote topic you proposed to me — “Cybersecurity as a Foundation for Uganda’s Digital Transformation and National Resilience” — is, I hope you will agree, precisely what this conference’s theme

already promises. I have simply tried to honour it by tweaking it to *Trust by Design: Building a Cyber-Resilient Digital Economy for Uganda*, in this address.

Beneath that theme lies a proposition I want to leave with you this morning. Uganda's digital transformation will succeed only if finance, technology and trust advance together. Technology can accelerate transformation. Finance can turn that transformation into investment, production and opportunity.

But trust is what allows citizens, businesses and institutions to participate with confidence — and cybersecurity is increasingly the principal means by which that trust is earned, and kept.

So the question before us is not simply how to keep intruders out. It is this: how do we build a digital economy that Ugandans can trust, that businesses can rely on, that investors can believe in, and that the economy can depend upon — even when systems come under stress? That is the question I want to explore.

Let me be plain about why this matters to a central bank. Trust is not a soft virtue added on top of sound economics; it is infrastructure — as real, and as load-bearing, as a road or a power line. Remove it, and every investment we make in connectivity, financial inclusion and digital government sits on ground that can give way without warning. That is why we treat cybersecurity this morning not as an IT agenda item, but as a macroeconomic one.

The stakes

Let me be direct about the scale of what we are discussing. Uganda's digital footprint is expanding rapidly — an estimated 23 million Ugandans, nearly half our population, are now online, driving commerce, financial inclusion, education and government service delivery. Our Digital Transformation Roadmap 2023/24–2027/28 aims higher still: 90 percent broadband coverage and 90 percent of citizens accessing e-services online by 2040. That ambition is the right one. But every gain in reach is also a gain in exposure.

The Uganda Police Force's Annual Crime Report records that reported cybercrime cases nearly doubled, from 245 in 2023 to 474 in 2024 — a rise of over 93 percent — before easing only slightly to 412 in 2025, still close to double the 2023 level, with associated financial losses running into billions of shillings each year.

A national assessment by NITA-U found that roughly four in every ten Ugandan small and medium enterprises have already experienced some form of cyberattack. Globally,

the picture is starker still: industry estimates now put the annual cost of cybercrime at some US\$10.5 trillion a year — a sum that, were it a national economy, would rank among the three largest in the world.

And the frontier of this risk is moving faster than our institutions can easily track. Barely weeks ago, the world learned — through disclosures from two of the world's leading artificial-intelligence developers — that autonomous AI agents had, without direct human instruction, breached production systems at a major technology company. I raise this not to alarm you, but to make a simple point: the tools available to both attackers and defenders are changing in real time. Whatever we resolve at this conference, therefore, cannot be a static resolution; it must be a commitment to continuous adaptation.

This pace of change is precisely why cybersecurity can no longer be viewed as merely a technical issue. It has become a strategic national capability — one that underpins economic stability, protects critical infrastructure, safeguards public confidence, and ensures the continuity of essential services when disruption occurs. In today's interconnected world, national resilience is increasingly measured by our ability to anticipate, withstand, respond to and recover from cyber incidents.

Uganda is already laying the foundations for this capability. The National Cybersecurity Strategy 2022–2026 commits us to a whole-of-nation approach; and only weeks ago, Government launched the Updated National Information Security Framework 2026, providing public institutions with practical tools and minimum security controls. These are the right foundations. The task now is to turn them into everyday practice — across every institution represented in this room, not only those with a statutory duty to comply.

From institution to ecosystem

This brings me to a second point, one that changes how we should think about resilience itself. The power of digital technology comes not from individual systems but from the connections between them. A payment platform links banks, telecom operators, merchants and consumers. Digital identity links citizens to dozens of services at once. Cloud infrastructure links many institutions to common providers. That interconnectedness creates enormous value — and it is also precisely how disruption travels. A vulnerability in a telecommunications network can surface as a crisis in financial services. A compromise of one identity credential can open doors across an entire ecosystem.

Engineers have long known that a network's strength lies not in any single node but in how failure propagates between them — a lesson financial regulators learned at great cost in 2008, and one cybersecurity is now teaching every other sector afresh. The relevant unit of resilience, then, is no longer only the institution. Increasingly, it is the ecosystem. The question each of us must ask is not only “is my institution secure?” It is: how secure is the network of institutions on which mine depends — and on which others now depend on me?

For the Bank of Uganda, this is not an abstraction. Financial stability has always depended on capital and liquidity; it now depends equally on the availability, integrity and reliability of the systems through which financial activity flows. Our supervisory work looks beyond individual balance sheets to system-wide vulnerabilities and interconnections, precisely because a cyber incident that begins as a technical failure can, within hours, become a payments disruption, a loss of confidence, and — if we are not prepared — a financial-stability event. That is why, effective December 2024, the Bank issued Cyber and Technology Risk Management Guidelines requiring every supervised financial institution to build robust governance, data-protection and security controls into their operations, backed by supervisory enforcement.

And it is why the Bank's own information-security programme is aligned to international standards, including ISO/IEC 27001¹, under executive and board oversight. Our most recent Financial Stability Review identifies cyber threats and system vulnerabilities as continuing operational risks to the sector — a finding we take as a standing instruction to ourselves, not merely an observation about others. We do not ask of the sector what we are not prepared to demonstrate ourselves.

No serious institution can assume it will never face an incident. The more useful question is: how well prepared are we when prevention fails? That is the discipline of resilience — the capacity to anticipate, withstand, detect, respond, recover, and, critically, to learn.

We do not design financial systems on the assumption that shocks will never occur; we hold capital buffers and run stress tests precisely because we know they will. Cyber resilience deserves the same rigour.

¹ ISO/IEC 27001 is the international standard for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). It provides the management framework and controls through which an organisation systematically identifies and manages those risks.

Three shifts

Ladies and Gentlemen, let me now turn to how we might operationalise the three foundational principles of my remarks today: collaboration, resilience and trust.

The first shift is from parallel effort to **Collaboration** as a capability. Threats do not respect institutional boundaries; our defences cannot either. That means stronger mechanisms for threat-intelligence sharing, coordinated incident response, joint cross-sector exercises, and — where it matters most — a shared, appropriately calibrated baseline of resilience across every institution connected to Uganda's critical digital ecosystem. I would put a challenge to this room: the rigour we now require of banks under our Cyber and Technology Risk Management Guidelines should not remain a banking-sector achievement alone. Telecommunications, government agencies and utility providers all have good reason to speak the same language of security, even where the regulatory mandate that governs them differs.

The second shift is from **Resilience** as compliance to resilience as practice. A framework filed away in a drawer is necessary but not sufficient. I would ask every leader here to pose the uncomfortable questions before a crisis, not during one: What happens if our primary system fails? If our key technology provider is unavailable for a day? If several institutions are hit simultaneously? Who decides, who communicates, who coordinates — and how quickly can we restore what matters most? A continuity plan nobody has rehearsed, a backup nobody has restored, is not yet a capability. It is a hope written down on paper. These are the questions that separate the prepared from the merely compliant.

The third shift is treating **Trust** as the outcome by which we judge ourselves — not the number of policies we hold, nor the firewalls we have bought, but whether citizens and businesses genuinely believe the systems they depend on are safe, reliable and accountable. Trust is not an intangible. It has economic value: it is why a citizen adopts a digital public service, why a business commits capital to a digital platform, why an investor backs our markets with confidence rather than caution.

And because trust, once lost, is far costlier to rebuild than to protect in the first place, safeguarding it is not a defensive expense. It is an investment in the credibility of our entire digital economy.

There is sometimes a temptation to frame our choice as one between security and innovation. That is the wrong choice. The real choice is between innovation that is trusted and innovation that is fragile; between growth that compounds over years and

growth that can be halted by a single avoidable shock. Security, properly understood, is not the tax we pay for innovation.

It is one of the conditions that makes innovation sustainable — which is why the principle I would leave with this conference is simple: build security in; do not bolt it on. Whether we are building a payment platform, a digital identity system, or deploying artificial intelligence in public services, security, privacy and responsible governance belong in the design from the first day, not the review that follows after something goes wrong.

A national compact

As this inaugural conference opens, perhaps its most useful outcome would be a shared national compact, built on three commitments: that we will not let institutional boundaries become gaps through which risk travels; that we will judge our preparedness not by our ability to prevent every incident but by our ability to withstand, recover and learn from the ones we cannot prevent; and that we will measure our digital transformation, ultimately, by whether Ugandans trust it enough to build their futures upon it.

Uganda's digital future will not be secured by technology, regulation or investment alone. It will be secured by institutions, systems and people choosing, deliberately and repeatedly, to work together. Let us secure by design, collaborate across boundaries, and build resilience before the crisis arrives — so that when disruption comes, as it will, we absorb it, we recover, and we emerge stronger.

This collective responsibility must begin with leadership. Cybersecurity is no longer solely the responsibility of ICT departments; it is a boardroom issue, an executive leadership responsibility, and increasingly a matter of national policy.

Every leader represented here has a duty to ensure that cybersecurity is firmly embedded in governance frameworks, investment decisions and organisational culture.

I congratulate the Uganda Communications Commission and all partners once again for convening this inaugural conference. I wish you fruitful deliberations.

For God and My Country.