The RiskEcho

ISSUE 10 - JANUARY 2026

Intriguing Insights

EXCLUSIVE INTERVIEW WITH MR. KENNETH OWERA
Chief Investment Officer, National Social Security Fund

HOW PROACTIVE RISK MANAGEMENT BECAME THE CORNERSTONE OF NSSF'S DIGITAL TRANSFORMATION

TEEN SEXTORTION & DEEPFAKES
A PARENT–COMMUNITY PLAYBOOK

AI, THE DOUBLE-EDGED SWORD

Making lives better.

NSSF a better life | 40 Years Making Lives Better

FOREWORD

To all our esteemed readers of ***The Risk Echo*** magazine, Happy New Year. May the new year open new doors for you, and may you achieve your aspirations – Amen!

We look forward to the new year, 2026, with a lot of excitement and expectations, as we wait to see the landmark event of the start of production of oil in the country- Insha'Allah! No doubt, oil production is going to be a game changer.

That aside for a moment, reflecting on the past year; out of the 365 days of 2025, one day that any member of the National Social Security Fund cannot forget is September 22, 2025; the day the Minister of Finance, Planning and Economic Development, Hon. Matia Kasaijja declared interest to members of 13.5%! This was, by any measure, a high return to members, which put smiles on their faces, according to the feedback we have received.

The performance was phenomenal; assets under management grew by 17.5% from UGX22.13trn to UGX26trn, gross realized income increased from UGX3.18trn to UGX3.52trn, while expenses ratio declined from 1% to 0.89%, reflecting increased operational efficiency. At 88% and 91% customer and employee satisfaction rates respectively, these were high by any standard.

This phenomenal performance shows our commitment to not only creating value but preserving it. The excellent performance is a key indicator of our robust risk management.

The ultimate measure or indicator of effective risk management is the extent to which an organization attains its objectives. As defined by ISO 31000, "risk" is the effect of uncertainty on an objective, whether positive or negative. That means the major determinant of achieving organizational objectives is the effectiveness of risk management.

In business, risk-and-return decision is the most critical one; as the saying goes, "the higher the risk, the higher the return". Our natural inclination as human beings is to avoid risk, especially high risk. But that also means missing out on the potential high reward/return! On the other hand, taking on risk, especially high risk, means contending with a potential for significant losses. So, striking a balance becomes the most critical decision you make in business, which can break or make you.

Finally, before you make a key decision, figure out what could go wrong, what would be the impact, and how you could minimize the impact.

Edward Senyonjo
Chief Risk Officer, NSSF

13.5%
Interest Declared

Assets Under Management
17.5% ▲ From **UGX 22.13trn** to **UGX 26trn**

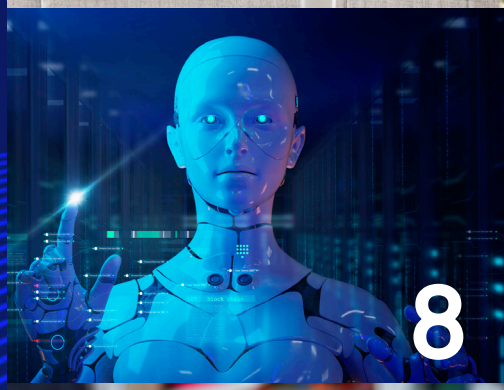
Gross Realized Income
▲ From **UGX3.18trn** to **UGX3.52trn**

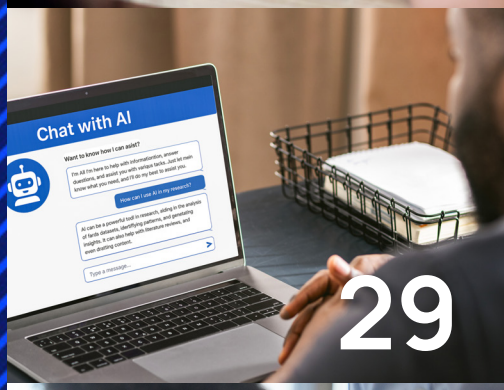
Expense Ratio
▼ From **1%** to **0.89%,** reflecting increased operational efficiency

Customer Satisfaction 88%

Employee Satisfaction 91%

CONTENTS





The Risk Echo is delighted to bring you an exclusive interview with

MR. KENNETH OWERA

Chief Investment Officer, National Social Security Fund

Qn: Mr. Owera, can you introduce yourself to our esteemed readers of The Risk Echo?

Thank you, and it's a pleasure to be featured in The Risk Echo.

My name is Kenneth Owera, and I currently serve as the Chief Investment Officer at the National Social Security Fund (NSSF) Uganda. I am an investment professional with over 15 years of experience, spanning pension fund management, infrastructure financing, capital markets, and strategic asset allocation.

My passion is building resilient investment portfolios that deliver sustainable long-term value for our members, while contributing meaningfully to Uganda's socio-economic transformation.

Qn: What is the role of a Chief Investment Officer at the Fund?

The Chief Investment Officer (CIO) provides strategic and operational leadership for the entire investment function of the Fund that manages over UGX 27.7 trillion (USD 7.4 billion) in assets across fixed income, equities, and real estate.

This involves:

i. Designing and implementing the Strategic Asset Allocation that guides how member savings are invested.

ii. Ensuring that the portfolio meets the Fund's objectives of safety, liquidity, and return.

iii. Leading due diligence, risk assessment, and investment execution for major transactions.

iv. Managing relationships with key stakeholders such as regulators, government agencies, development partners, and private sector players.

v. Overseeing investment governance, monitoring, performance reporting, and risk management across all asset classes.

In short, the CIO ensures that every shilling of member savings is invested prudently, responsibly, and sustainably.

Qn: The Fund declared an interest to members of 13.5%; this is a very good return for members by any measure. How did you manage to achieve this amidst challenging economic times?

Delivering a 13.5% return in such a volatile environment required discipline, agility, and strong execution.

A few success factors were critical:

i. A resilient portfolio structure

Our strategic allocation - 80% fixed income, 14% equities, and 6% real estate - helped us navigate geopolitical and trade related challenges, inflationary, and interest-rate swings, while preserving capital.

ii. Timely decision-making

We took advantage of high-yielding government securities in a timely manner, before rates started normalizing.

iii. Strong equity performance

Regional listed equities, particularly in Kenya and Tanzania, recovered strongly after the pandemic-era downturn.

Delivering a 13.5% return in such a volatile environment required discipline, agility, and strong execution.

iv. **Improved efficiencies and cost management.**

Through better governance, prudent investment decisions, and reduced operating costs, we maximized the value for members.

v. **A robust risk-management framework.**

This allowed us to make informed decisions and manage uncertainties more efficiently.

Ultimately, it was a combination of strategic foresight, operational discipline, and a committed investment team.

Qn: At about $7.4bn of assets under management, the NSSF Uganda is the largest pension fund in the whole of East Africa. Tell me, what is the secret of your performance?

There is no secret, but rather a consistent culture of discipline and governance. The Fund's success rests on three pillars:

1. **Long-term investment discipline**

We invest with a long-term outlook, enabling us to weather short-term volatility and capture long-term value.

2. **Strong governance and accountability**

Every investment decision passes through rigorous management and Board scrutiny, supported by data analytics, research, and risk assessment.

3. **A high-calibre, professional investment team**

Our team combines global best practice with local expertise, ensuring we respond to market dynamics with precision.

Our mandate is simple - protect workers' savings and grow them sustainably. That clarity of purpose drives our performance.

Qn: The NSSF investment portfolio is significantly skewed towards government securities- close to 80%. Financial analysts believe that when the country starts producing oil, the government may reduce borrowing, and hence, the interest rates will decline. How likely are you to sustain a double-digit return to members?

Yes, we are confident about sustaining strong returns - even as the macroeconomic environment evolves.

While government securities currently anchor the portfolio and the Fund's performance, we are actively seeking opportunities in higher-value sectors, including:

i. Regional listed and unlisted equities

ii. Infrastructure opportunities in energy and transport

iii. High-quality innovative real estate developments

iv. Alternative investments that provide inflation-hedged and uncorrelated returns.

The oil economy will create new opportunities in logistics, services, infrastructure, and financial markets. Should interest rates decline, equity markets will typically be expected to strengthen, creating upside for the Fund.

The essence of good portfolio management is adaptability - and

Temangalo is one of the affordable housing projects by NSSF Uganda.

we continue to identify the right opportunities to reposition the portfolio for the next decade of economic transformation.

Qn: The NSSF is a significant player in the real estate sector but the houses you build are for the high-end market, where majority of your members don't belong. Do you have any plans for affordable houses?

Absolutely. Affordable housing is a key strategic priority for the Fund, and we are actively pursuing viable solutions to deliver it sustainably.

Looking ahead, the Fund is developing a comprehensive real estate strategy that creates a clear pathway for delivering affordable and mid-income housing on large scale. This includes exploring higher-density designs, cost-effective construction methods, and mixed-use developments that optimize land utilization and reduce unit costs.

In addition, the Fund's other initiatives - such as Amaka - are designed to complement this shift by enabling members to save specifically towards homeownership, thereby expanding the pool of potential buyers for more affordable units.

We are also positioning the Fund to play a catalytic role by partnering with government, development finance institutions, and private developers to crowd in additional capital and expertise. These partnerships will be critical to delivering affordable housing at price points that are accessible to ordinary Ugandans and our members, while still maintaining the commercial integrity required of a pension fund.

Qn: If I want to buy a house, say in Temangalo, what are the terms?

Our real estate sales are designed to be transparent, equitable, and customer friendly. Once selling of the Temangalo Housing Project commences, the Fund will provide comprehensive guidance on pricing, buyer eligibility, and the sales process, to ensure a smooth and well-structured experience for all prospective purchasers.

Qn: What are some of the key challenges that you face in the investment process at the Fund and how do you address them?

At macro level, our challenges stem from the structure of the economy, mainly the limited depth in local capital market and macroeconomic volatility, typical characteristics of emerging markets, while at operational level we contend with regulatory bottlenecks.

We undertake various measures to minimize the impacts of these challenges on the business, including but not limited to:

i. **Limited depth in local capital markets.**

   We address this through regional diversification and selective private equity and infrastructure investments.

ii. **Regulatory bottlenecks: Delays in regulatory approval.**

   We work closely with regulators and government institutions to improve turnaround time, while ensuring compliance.

iii. **Macroeconomic volatility.**

   Our risk-management framework includes stress testing, scenario analysis, and active portfolio management, which help to reduce variability between expected and actual returns on investment.

iv. **Internal project implementation delays**

   We are strengthening project governance and contract management to ensure timely execution.

Despite these challenges, our disciplined processes ensure we consistently deliver value for members.

Qn: What is the last and most important message you would like the NSSF members to take away?

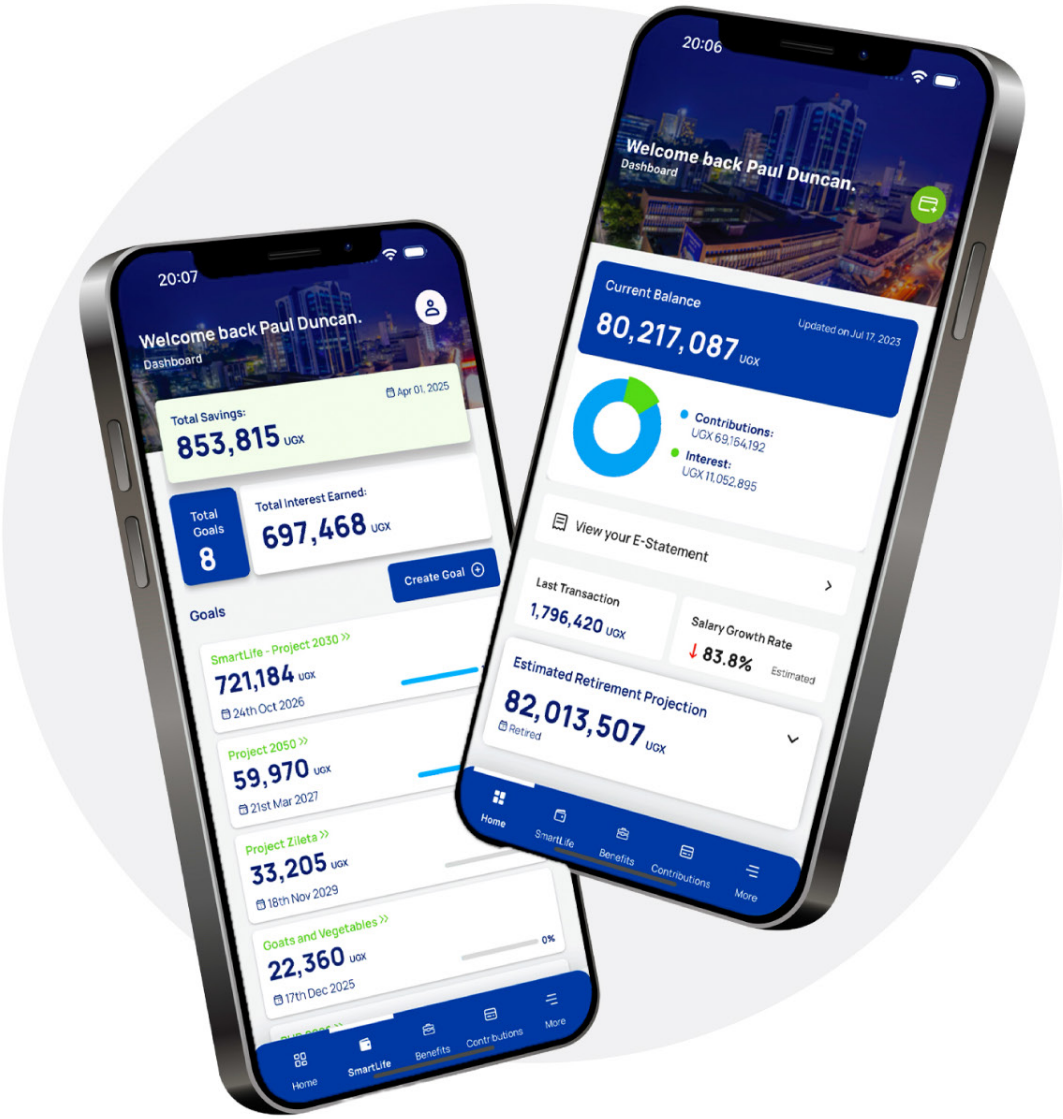
Your savings are safe, they are growing, and they are working for you.

At NSSF, every investment decision is guided by one principle: Protect and grow the savings of the members. We remain committed to transparency, professionalism, and delivering competitive long-term returns.

We thank our members for their trust, and we encourage everyone to save with the Fund by taking advantage of the newly introduced voluntary saving option – The Smartlife product. Thank you. ■

Fresh Look, Seamless Experience

Enjoy smooth and easy access to all our services with the redesigned **NSSFGo** App.



GET IT ON Google Play

Download on the App Store

NSSF a better life | 40 Years Making Lives Better

DIGITAL DNA

THE INVISIBLE FOOTPRINT THAT IS LIKELY TO COMPROMISE YOUR PRIVACY

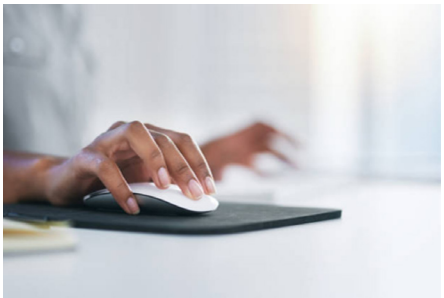
Jesse Okutre
Operational Risk Specialist, NSSF

Imagine this:

A video montage of every single thing you have ever done online is about to play on a giant screen at public square! I am talking about your secret late-night cake recipe searches, the embarrassing meme you liked from 2014, that oddly specific deep dive search into the migratory patterns of the wildebeest in Northern Tanzania; be it on google, Facebook or TikTok. Still not bothered, you must be crazy!

Welcome to the world of your Digital DNA, the invisible, ever-evolving footmark you have been building since the first time you started using the computer and internet.

In the Digital age, every click, search, post, like, comment and share contribute to a unique online identity known as "Digital DNA."



This invisible footprint encapsulates an individual's online behavior, preferences, and interactions across platforms. As technology advances, Digital DNA is increasingly being used to evaluate individuals in contexts like hiring, visa applications, social interactions, as well as companies sending adverts to your pages and browsers as you surf through the web.

This article explores the current state of Digital DNA, its future implications, and why individuals must exercise caution to protect their online reputation.

What is Digital DNA?

Digital DNA refers to the cumulative record of an individual's online activity, including social media posts, search histories, comments, shared content, and even metadata like location tags or IP addresses. Unlike physical DNA, which is static, Digital DNA evolves with every Digital interaction: that one angry comment you left on a news article, that one google search about the direction to Workers House - all sequenced. It paints a picture of your personality, beliefs, habits, and affiliations; often revealing more than you might intend and it is being used to judge you in ways that might surprise or terrify you. Currently, Digital DNA is collected through various means, including:

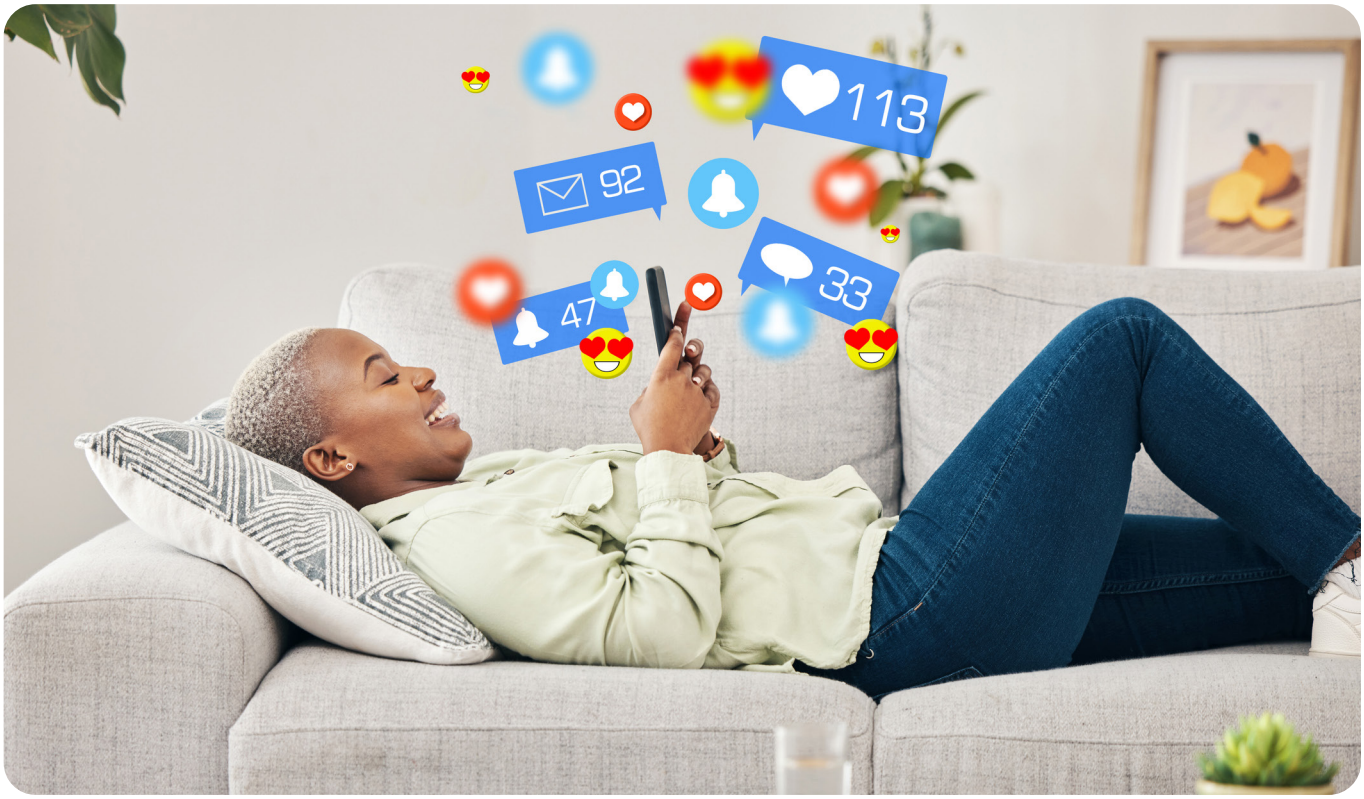
i. **Social media platforms:** Posts on X, LinkedIn, Instagram, Facebook, TikTok and others form a public-facing profile.

ii. **Cookies and tracking:** Websites track browsing habits, purchases, and preferences. These cookies are used to send adverts to the webpages you are browsing through.

iii. **Data aggregators:** Companies compile data from multiple sources to create comprehensive profiles.

iv. **Public records:** Online records of legal, registration bureaus, financial institutions, School or University data/websites, or professional activities (articles, theses, etc.) contribute to the footprint.

Data from these sources is often analyzed using Artificial Intelligence (AI) and machine learning to generate insights about behavior, reliability, and character of an individual.



Current uses of Digital DNA

Digital DNA is already a critical factor in decision-making processes across sectors, e.g. hiring, marketing, visa applications, etc. Here are the ways in which your Digital DNA is being used:

i. **Recruiting employees-the creepy interviewer.**

Employers are increasingly screening candidates' digital DNA to assess cultural fitness, professionalism, and potential risks. In 2023, Career Builder survey found that 70% of employers check candidates' social media profiles to establish if these candidates would fit in their organizations. A simple name search in google can reveal a lot about a potential candidate, who is on LinkedIn, Snapchat, Facebook and other social media accounts where information can easily be picked about them.

ii. **Visa and immigration applications-the digital border guard.**

Governments use Digital DNA to evaluate applicants' credibility and security risks. The U.S. Department of Homeland Security, for example, requires visa applicants to disclose social media handles as part of the vetting process. In 2025, the visa for Bob Vylan, a member of the British punk rock group, was revoked after a review of his social media posts revealed chants criticizing the Israel Defense Forces (IDF) in relation to the Gaza-Israel war. The band was considered a security threat since there were already protests in the US about the war.

iii. **Personal and social contexts-the algorithmic matchmaker**

Individuals and organizations use Digital DNA to assess trustworthiness or compatibility. For example, dating apps like Bumble and Tinder integrate social media data to verify user identities or highlight shared interests. In China, the social credit score run by the People's Bank of China compiles data on borrowing history, bill payments, and other financial transactions. This information gathered is analyzed and it is the basis used for advancing loans to small business owners.

iv. **Marketing and targeted adverts-the adverts that follow you everywhere.**

Have you ever talked about or searched about wanting a chicken tikka pizza and then immediately gotten a café java or food hub advert popping up? That is not a coincidence; it is your Digital DNA at work. Companies use your search history, location data, and even conversations picked up by your smart devices to serve you hyper-targeted adverts. So, when you allow applications on smartphones to receive calls during setup, know there is someone intending to listen into your conversations (does the US $3.45 billion fine by European Union to Google ring a bell?)

The future of digital DNA

As technology evolves, the scope and impact of Digital DNA will expand significantly

AI-driven profiling: Your life, judged by an algorithm.

AI-driven profiling leverages machine learning algorithms to process data which generates information with

precision from diverse sources such as social media, financial transactions, location data, browsing history, and even biometric information to generate predictive models or "Digital DNA" for individuals.

These profiles enable organizations to categorize people for specific outcomes, such as creditworthiness, security risks, or consumer preferences. Let's take the case of Ismail Ajjawi, a Palestinian student who was initially denied entry to the U.S. to attend Harvard. Why? Because of his friends' social media posts. That's right, you might now be judged by the company your Digital DNA keeps. So maybe it's time to finally unfriend that cousin or friend who posts conspiracy theories about aliens building the pyramids.

Immutable decentralized records: The internet never forgets.

Immutable decentralized records refer to data stored across a network of computers rather than a central authority, making it impossible to alter, delete, or tamper with once it has been verified and recorded. This is achieved through cryptography and consensus mechanisms.

This permanence makes the system ideal for applications requiring trust, transparency, and security, such as financial transactions, identity verification, supply chain tracking, and credit scoring. This is already happening in finance. In Uganda, companies like Tugende, use a cloud-based database system developed in-house, inspired by this architecture to record microloan repayments for motorcycle (boda boda) riders.

This creates a secure and lasting credit history, allowing people with no formal banking history to prove they are trustworthy. Similarly, Stanbic Bank Uganda partners with technology startups to secure financial data for loan approvals.

Global Standardization: One Digital profile to rule them all.

Right now, your data is scattered across a million different servers. In the future, countries and corporations might just decide to put it all together in one giant, unified database. Imagine a global Digital DNA database for visa and loan applications, etc. One streamlined check that shares your data across borders. Interpol already uses a unified database for law enforcement; this could spread to travel, banking, and employment.

Personalized marketing and manipulation: Not just adverts anymore.

You know how you search about a Mazda CX 3 and then get followed around the internet by adverts on TikTok, Facebook, X, etc. about that car for weeks? That was just the training wheels. In the future, personalized manipulation will be so advanced, it will feel like the internet can read your mind (because, in a way, it can).

You will find that the jobs offer will be tailored to your deepest insecurities, experience and desires, political messaging campaigns will micro-target you based on your deepest fears and hopes inferred from your Digital DNA, and your social media feed will be a perfectly crafted echo chamber, designed just for you.

And lastly, dynamic pricing could extend beyond flights and Ubers; online stores might see from your Digital DNA that you are a desperate, last-minute shopper and charge you extra for that birthday gift you are desperately looking for.

Digital footmark used in courts of law: The truly scary part.

Looking even further ahead, your online activity could start influencing legal proceedings. A prosecutor could use your aggressive gaming chat logs, offensive posts and comments, YouTube view history to argue you have a violent temperament? Or intend to cause harm? Could your paranoid search history be used against you in court? It's a legal and ethical minefield that we are only just beginning to map.

Why individuals must be cautious?

Think of your Digital DNA as a permanent, public passport to your life. It can grant you access to amazing opportunities, dream jobs, travel visas, exciting connections, but one wrong stamp on that passport is a single ill-considered post, like, or share can just as easily get you denied entry at the border permanently.

Permanence: Digital footprints are permanent.

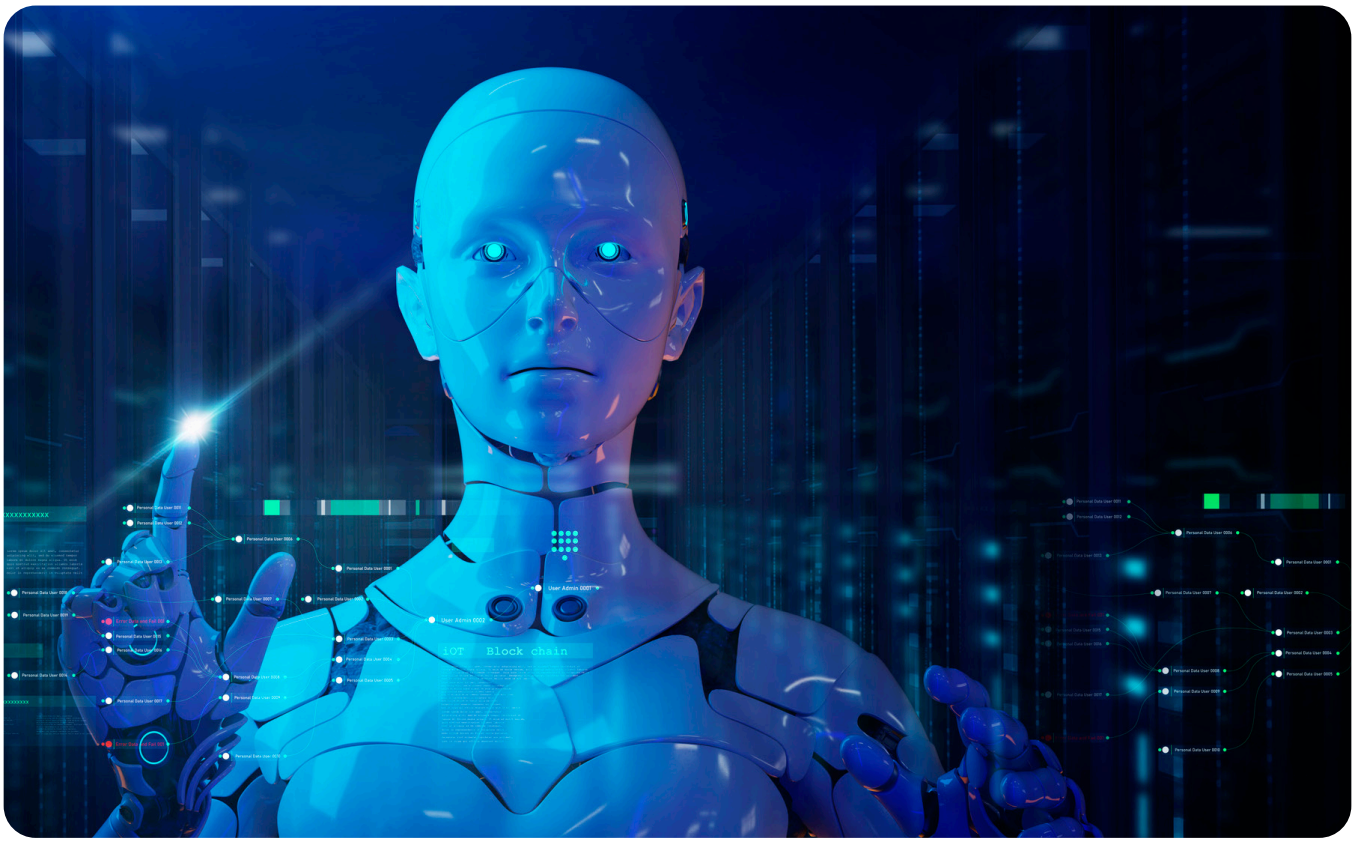
You have heard the saying, "the internet never forgets" this isn't just a cute phrase, it is a blunt reality. That post you delete in a moment of panic, it has already been archived, screenshotted, or cached by someone or something. There is no true "delete" button online. Your Digital DNA is a tattoo, not a temporary sticker. You can try to laser it off, but the scar will always remain.

Context misinterpretation: Your sarcasm doesn't translate.

Remember that brilliantly sarcastic meme you shared in 2015? Yeah, an AI scanner or a future hiring manager in 2025 won't get the joke. Without the original context of your friend group, the inside joke, or the trending topic, your content can be wildly misinterpreted. A sarcastic joke becomes a serious statement, and an edgy joke could become a glaring red flag ("I don't want peace, I want problems, always", common meme could be misinterpreted by parents). As AI improves, it gets better at scanning but often worse at understanding human nuance, making you vulnerable to being judged by a humorless algorithm.

Data breaches: Your secrets are only as safe as the weakest link.

You might be careful, but are the companies holding your data careful? The 2015 Ashley Madison breach is the classic horror story, where leaked private interactions led to public shaming, divorces, and ruined careers. You can have the most locked-down and pristine social media profile in the world, but if a platform you use gets hacked, your private direct messages, search history, and hidden interactions, can be spilled for the world to see. Your Digital DNA is not just what you show, it is also what you trust others to keep safe.



Algorithmic bias: When a robot decides you are a risk.

The AI systems that analyze your Digital DNA are built by humans, and they inherit human biases and tendencies. These systems can misjudge you based on incomplete or skewed data. For example, maybe your online activity shows you are job hopping, but the algorithm doesn't see you pursuing better opportunities or perhaps your network includes controversial figures, so the AI will unfairly flag you by association. You are not being judged by a person who can understand your story, but by a code that reduces your life to a risk score.

How to protect your Digital DNA: A practical survival guide

Audit your digital closet.

Regularly review your social media accounts for outdated or inappropriate content, use tools like Google Alerts to monitor mentions of your name online, it's like having your own personal internet detective. Unfollow friends who post offensive comments, and those who keep tagging you on controversial debates and opinions.

Think before you post!

Avoid sharing controversial opinions, offensive humor, or personal details that could be misinterpreted.

The good rule of thumb is: Ask, **"Would I say this in a job interview or explain it comfortably to my spouse?"**

Lock your digital doors

Use privacy settings to restrict who can view your posts and status, tag you, add to groups, or see your friends list. Always enable two-factor authentication (2FA) to prevent hackers from accessing your accounts.

Keep your story straight.

Always update your LinkedIn, X, and other public profiles to align with your current resume and professional persona. Discrepancies in job titles, dates, or qualifications are red flags to employers or if you cannot keep up with updates, delete those accounts.

Build a positive digital DNA.

Proactively share content that reflects your values, expertise, and professionalism. Comment thoughtfully on industry articles, share your own projects, and engage in constructive conversations. This builds a positive footprint that overshadows any old, irrelevant content.

Finally

Digital DNA is no longer a passive footprint but an active component of personal identity. As technology advances, it could enable automated ranking, mass surveillance, and manipulated content, making careless online activity costly. To mitigate these risks and build a professional advantage, individuals must proactively audit their Digital footprint, enforce strict privacy, and engage in authentic online behavior. ■

DIGITAL TRUST

THE NEW CURRENCY IN AN AGE OF UNCERTAINTY

Norbert Namanya
Information Security Specialist, NSSF

> **Trust takes years to build, seconds to break, and sometimes never quite recovers.**

You're scrolling through TikTok and suddenly bump into a video of a well-known CEO; suit on, smile wide hyping up the "next big investment opportunity" that suspiciously sounds like a pyramid scheme. For a second, you wonder, could this actually be real? Your fingers itch to forward it to your "#TeamNoSleep" WhatsApp group, or better- still to that "#SuperPerformers" group at work. After all, being the first to drop "hot news" has its perks... instant credibility, bragging rights, may be even a few laughing emojis.

But something inside whispers, hold up... so you pause. Hours later, you find out the video was nothing but an AI-generated deepfake cooked up by shady actors trying to bait the gullible. That pause just saved you a lot of embarrassment from spreading fake news, tarnishing your reputation, and perhaps even becoming part of the scam's statistics.

Sounds dramatic? Not really. This is the digital reality we're living in. Between artificial intelligence, deepfakes, and the wildfire speed of social media, the line between truth and trickery is now paper-thin; and the biggest casualty is trust.

Here's the thing; digital trust isn't just a cybersecurity jargon or another fancy buzzword tech people throw around. It's the quiet confidence we all lean on in the belief that what we see, read, and interact with online is genuine, secure, and reliable. For you and me, it's knowing the news article isn't fake, the mobile money transfer will land, and the video of your favourite artist isn't an AI parody.

For organizations, it's far bigger; including protecting sensitive data, ensuring their systems don't get compromised, and making sure customers never doubt their integrity.

In this article, I break down why digital trust is becoming the new currency of the modern world, helping us survive fake news, guarding our personal data, and enabling organizations to build lasting credibility in an age where skepticism runs high.

Guarding Against Misinformation

The challenge of misinformation is no longer limited to blurry WhatsApp forwards. With the rise of AI, today's fake content is dangerously convincing. Deepfake videos mimic public figures with oddly strange accuracy, while AI tools generate fabricated articles and recordings. Ordinary users are left questioning the legitimacy of nearly everything they consume online.

This confusion has real consequences. A fake financial tip could trick someone into losing their savings. A fabricated political video could spark unnecessary social tension. Even a false rumour about a brand could ruin its reputation overnight.

Digital trust, at personal level, means pausing before clicking "share". It means checking multiple sources, using fact-checking platforms like Africa Check or PesaCheck, and applying simple tools such as reverse image searches, a technique used in identifying the source of an image, verifying its authenticity, finding similar content, and discovering instances of copyright infringement or misuse. By exercising caution, we protect ourselves and shield our networks from falsehoods.

Digital trust does not happen by accident. It is deliberately built and consistently reinforced. For individuals, this starts with digital literacy and ability to resist the urge of wanting to be the first to share "hot gossip". Fact-check tools and authenticity markers are shields against misinformation every day.

> Every time we pause before forwarding unverified content, we strengthen digital trust in our communities.

Digital Trust in Organizations:

For organizations, digital trust is not optional, it is a must-have. Every customer who signs up for a service, every employee who shares personal data, and every supplier who connects to your system is silently saying, "I trust you to protect me." When that trust is broken, the consequences are often more devastating than the breach itself.

In Uganda, the Data Protection and Privacy Act of 2019 makes this responsibility legally binding. Organizations are expected to collect, process, and store personal data securely and fairly; whether it's National IDs, Social Security Numbers, medical records, or financial transactions. A single leak of this sensitive information doesn't just trigger regulatory fines, it can wipe out years of brand equity and invite scrutiny from the public, media, and regulators.

True digital trust in an organizational setting rests on three foundational pillars:

i) Data Security and Privacy

Protecting data is non-negotiable. Encryption, strong access controls, and regular patching are the basics. Beyond that, leading organizations invest in tools such as dark web monitoring, threat intelligence, and proactive detection of compromised credentials to catch breaches early.

ii) Transparency and Communication

Breaches will happen. What distinguishes a trusted organization is not perfection but honesty. Communicating incidents promptly, clearly, and with accountability reassures stakeholders that the organization values integrity over image. Silence or cover-ups only deepen suspicion.

Governance and Accountability

Digital trust must be championed at board and executive levels, not treated as an IT project. Regular audits, alignment with international standards like ISO/IEC 27001, and clear accountability structures demonstrate that security and privacy are strategic priorities.

Above all, trust is human-centered. Employees can either be the weakest link or the strongest shield. Organizations that continually invest in staff awareness programs, from phishing simulations to training on responsible use of AI, empower their people to become defenders of trust rather than risks to it.

In the end, digital trust is not about technology alone, it is about culture, leadership, and consistent action. Organizations that embed trust into their 'DNA' not only comply with laws but also win loyalty in a marketplace they operate where reputation is everything. Those that fail, risk irrelevance or worse still, wipe-out.

Conclusion:

In today's uncertain digital world, trust has become the most valuable currency. For individuals, it's the difference between falling for fake news and confidently navigating online spaces. For organizations, it's the deciding factor between loyalty and abandonment.

Digital trust is not built overnight but it cannot be ignored. By consciously investing in secure systems, transparent communication, and responsible digital behaviour, we can create digital ecosystems where truth prevails over manipulation, and confidence replaces doubt.

In the digital age, once trust is broken, repair may be impossible. That is why we must prioritize digital trust today before it is too late.

THE DIGITAL BAZAAR

A NEW PARADIGM FOR TRADE AND INVESTMENT IN EAST AFRICA

Daniel Otim
Entrepreneur, M&E expert & Statistician

Twiga Foods platform connects smallholder farmers to urban retailers.

The narrative of global e-commerce, often defined by Western models of consumer convenience, is being fundamentally rewritten in East Africa. Here, digital trade is not merely a channel for retail; it is a strategic, mobile-first overhaul of foundational economic structures. This evolution presents a unique case study in market adaptation, financial technology convergence, and the formalization of informal sectors, offering distinct opportunities and challenges for the discerning investors and policymakers.

A Foundational Shift: East Africa's trajectory bypassed the traditional sequence of broadband and credit card proliferation. The catalyst was the mobile money revolution, ignited by the launch of M-Pesa in Kenya. This established a pre-existing framework of digital trust and financial inclusion, with over 70% of the adult population in key markets actively using mobile wallets. Consequently, e-commerce platforms entered an ecosystem already primed for digital transactions, allowing them to focus on solving critical supply chain and logistics inefficiencies rather than building payment infrastructure from scratch.

This leapfrog effect created fertile ground for innovation, with platforms developing solutions tailored to the region's specific pain points.

The Core Engine: B2B e-commerce and supply chain formalization. While consumer-facing platforms capture headlines, the most profound impact is occurring within the Business-to-Business (B2B) sector. These platforms are addressing systemic inefficiencies in the region's largely informal economy, which accounts for approximately 80% of trade. The few examples include;

Wasoko: Operating across six African nations, Wasoko digitizes procurement for informal retailers. By offering next-day delivery of essential goods, embedded financing, and data-driven insights, it enhances working capital efficiency and stabilizes supply chains for tens of thousands of small businesses.

Twiga Foods: This platform directly connects smallholder farmers to urban retailers. By disintermediating numerous layers of brokers, Twiga increases margins for producers, ensures quality consistency for vendors, and reduces price volatility for consumers.

These B2B ventures are effectively constructing a digital backbone for regional commerce, driving a gradual but significant formalization of trade.

Strategic Necessities: Navigating the Headwinds

Sustained growth is contingent upon successfully navigating several critical challenges. Key risks that demand careful mitigation include:

1. Operational & Logistical Fragility.

The high cost and unreliability of last-mile delivery, due to poor addressing systems and urban congestion, directly impact margins and scalability.

2. Cybersecurity and fraud exposure

The rapid digitization of commerce and payments creates an expanding attack surface for fraud, particularly in C2C transactions, necessitating robust investment in escrow systems and secure platforms.

3. Regulatory volatility

The regulatory landscape remains fragmented and evolving. Sudden changes in cross-border trade policies, data protection laws, or digital taxation can introduce significant uncertainty and compliance costs.

4. Competition and market saturation

Initial success in key urban centers leads to intense competition and market saturation, while expansion into peri-urban and rural areas presents its own profound logistical and unit-economic challenges.

Despite the above challenges, solutions are around the corner.

i. **The consumer landscape: Hybrid models and building trust.** The consumer e-commerce experience is characterized by hybrid models that can mitigate some of the risks outlined above. Pure-play online retailers face significant headwinds, leading to the rise of adaptable solutions:

ii. **Phygital Integration:** Platforms like Kikuu combine online marketplaces with physical pickup points, allowing for cash-on-delivery payments and in-person product inspection. This blended approach builds essential consumer confidence.

iii. **Social Commerce Proliferation:** WhatsApp, Facebook Marketplace, and Instagram have become de facto storefronts for micro-entrepreneurs. You have probably seen women advertising electricals while dancing on social media. These grassroots "digital hustler economy" leverages ubiquitous social platforms and mobile money to facilitate commerce with minimal overhead, though it operates with limited regulatory oversight.

iv. **Inventory Management System (IMS):** This is the cornerstone. Selling products you don't have (overselling), leads to canceled orders and angry customers, or having too much capital tied up in slow-moving stock (overstocking). Retailers are implementing IMS syncs in real-time with their e-commerce platforms. When a sale happens, inventory levels are automatically updated across all channels (website, Amazon, eBay, etc.)

Future outlook

i. **Sector-Specialization and Fintech Convergence.**

The next wave of innovation will likely be hyper-local and deeply integrated with adjacent sectors:

ii. **Agri-tech expansion**

Building on the existing models, future platforms will integrate access to inputs, insurance, credit, and real-time climate data, directly enhancing agricultural resilience and profitability.

iii. **Fintech-ecommerce symbiosis**

The convergence of financial services and digital trade will accelerate, manifesting in buy-now-pay-later (BNPL) schemes, credit scoring based on transaction histories, and the embedding of savings and insurance products within commerce apps.

Conclusion

East Africa's e-commerce ecosystem is not a derivative of foreign blueprints. It is a pragmatic, indigenous model built on the pillars of mobile money, adaptive entrepreneurship, and the strategic digitization of informal trade. For global stakeholders, the region offers a compelling insight into a future where trade is not solely defined by scale and speed, but by financial inclusion, supply chain resilience, and community-centric innovation. As these digital bazaars mature, they are poised to become powerful engines for sustainable economic growth and formalization across the continent. ■

HOW RISK CULTURE CAN BE A CATALYST FOR ORGANIZATIONAL RESILIENCE

Joshua Kibirige,
Operational Risk & AML Manager, NSSF

In a rapidly evolving risk landscape, organizations are constantly exposed to uncertainty - whether in the form of economic volatility, regulatory shifts, technological disruption, or geopolitical tensions. In such a dynamic environment, the ability to withstand shocks and recover from disruption is not only a competitive advantage; it is a business imperative. This is where risk culture plays a pivotal role.

Risk culture refers to the shared values, norms, attitudes, and behaviors within an organization that shape how risk is perceived, understood, communicated, and managed.

It, therefore, serves as a foundational element in securing organizational resilience by:

i. Ensuring leadership commitment and establishing a strong tone at the top

ii. Guiding decision-making

iii. Strengthening internal controls

iv. Enabling firms to respond swiftly and effectively in the face of adversity.

When these elements are embedded and consistently reinforced, the risk culture becomes a strategic asset - equipping the organization to better anticipate emerging threats, adapt to dynamic conditions, and recover with agility from adverse events. Rather than operating reactively, resilient organizations cultivate a proactive risk mindset, recognizing that risk is not only a challenge to be mitigated, but also a driver of opportunity, innovation, and long-term value creation.

This article, therefore, explores how fostering a strong and healthy risk culture from within serves as a critical driver of organizational resilience

Securing leadership commitment and establishing a strong tone at the top

A sound risk culture fosters strong leadership commitment, demonstrated through transparent communication, visible reinforcement of ethical standards, and a clear emphasis on accountability. Establishing this tone at the top is critical in shaping organizational attitudes toward risk, as it builds trust, encourages open and constructive dialogue, and promotes a culture of responsible risk-taking. When consistently upheld, these leadership behaviors embed risk awareness into the organizational fabric, enabling the organization to better anticipate, absorb, and recover from disruptions. Ultimately, this alignment between leadership and culture forms a cornerstone of organizational resilience.

Leaders who embody a strong risk culture are better positioned to foresee emerging threats, make informed decisions under pressure, and foster a climate of trust and agility.

As risk expert Norman Marks emphasizes, "An effective risk culture is the foundation for making informed and intelligent decisions under uncertainty."

For example, during the 2008 global financial crisis, JPMorgan Chase stood out as one of the few major financial institutions that maintained relative stability and resilience. This outcome was not coincidental, but rather the result of a deeply embedded risk culture reinforced by disciplined leadership. Under the direction of Chairman and CEO Jamie Dimon, the bank had a robust risk governance framework and a leadership team that prioritized long-term stability

over short-term profits. Unlike many of its peers, JPMorgan deliberately avoided excessive exposure to subprime mortgage-backed securities and maintained conservative credit standards.

This cautious approach was rooted in a risk culture that emphasized rigorous due diligence, robust oversight, and open challenge across all levels. Jamie Dimon personally engaged in risk discussions and encouraged dissenting views within the executive team, setting a clear and consistent tone at the top. As he noted in his 2009 shareholder letter: "We never changed our credit standards and always insisted on strong risk controls. It is our culture and discipline that protected us." This case illustrates how risk culture, when championed by leadership, can significantly enhance an organization's ability to navigate periods of severe stress.

Guiding decision-making

A well-established risk culture plays a critical role in guiding decision-making by aligning choices with the organization's risk appetite, values, and strategic goals. When risk awareness is embedded throughout the enterprise, decision-makers are more likely to move beyond short-term performance metrics and consider the long-term consequences and risk implications of their actions. This results in more balanced, informed, and forward-looking decisions.

For example, according to the Financial Crisis Inquiry Commission report (2011), in the period leading up to the 2008 financial crisis, Goldman Sachs made a strategic decision to substantially reduce its exposure to subprime mortgage-backed securities. This decision was driven by comprehensive internal risk assessments and supported by an organizational culture that promoted critical evaluation of emerging market conditions.

As a result, the firm was able to limit its financial losses and maintain operational stability, demonstrating a level of resilience that many of its industry peers, who suffered significant losses, were unable to achieve.

Embedding risk awareness in both strategic planning and operational execution enables organizations to anticipate threats, avoid excessive risk-taking, and respond quickly to emerging issues. In this way, risk culture becomes a powerful enabler of resilience.

Strengthening internal controls

Risk culture also plays a central role in strengthening internal controls - ensuring they are not viewed as mere compliance obligations, but as essential tools for managing risk proactively. In organizations with a mature risk culture, employees understand the rationale behind controls and take ownership of their role in maintaining them. This fosters a culture of vigilance, timely escalation of issues, and continuous improvement.

In the financial sector, firms with strong risk cultures often exceed regulatory requirements by embedding controls directly into business processes, leveraging real-time risk reporting, and promoting a "speak-up" environment where control breaches are reported without fear of blame. Such practices reduce the likelihood of operational failures, fraud, or regulatory breaches and enable early detection of risk exposures.

Ultimately, internal controls rooted in risk culture help build a resilient organization that can adapt to disruptions while maintaining operational integrity and stakeholder confidence.

Enabling firms to respond swiftly and effectively in the face of adversity

A well-embedded risk culture is foundational to enabling organizations to respond swiftly and effectively in the face of operational disruptions, cyber incidents, or broader crises. This cultural maturity directly supports the adoption and execution of Business Continuity Management (BCM) and Business Continuity Planning (BCP) strategies.

In firms where risk awareness is deeply ingrained, employees across all levels are not only encouraged - but expected - to identify, escalate, and act on emerging threats without fear of blame or organizational inertia. This proactive approach shortens response times and aligns naturally with Recovery Time Objectives (RTOs) by ensuring that critical business functions can resume within acceptable timeframes.

Organizations with mature risk cultures also prioritize preparedness through stress testing, scenario planning, and crisis response simulations - not just as formal exercises, but as integral parts of business thinking.

For example, during the early stages of Covid-19, several financial institutions with strong risk cultures were able to quickly activate business continuity plans, reallocate resources, and sustain critical operations with minimal disruption. Their ability to respond was not accidental, it was the product of a culture that values transparency, accountability, and readiness.

Ultimately, when risk culture supports proactive behavior and timely communication; organizations are better positioned to absorb shocks, make informed decisions under pressure, and recover with greater speed and stability - hallmarks of true organizational resilience.

Conclusion

In an era defined by constant disruption and complexity, cultivating a strong risk culture is no longer optional; it is a strategic necessity. As this article has shown, risk culture underpins organizational resilience by securing leadership commitment, guiding sound decision-making, reinforcing internal controls, and enabling rapid response during crises.

Ultimately, a strong risk culture is not just a safeguard, it is a catalyst for organizational resilience. ■

HOW PROACTIVE RISK MANAGEMENT BECAME THE CORNERSTONE OF NSSF'S DIGITAL TRANSFORMATION

Ritah Namulindwa
Business Analyst, NSSF

In an era defined by digital disruption and escalating fiduciary responsibilities, the National Social Security Fund (NSSF) has undertaken a strategic imperative to transcend conventional compliance and embed proactive risk management as the fundamental engine of its operational strategy.

Recognizing that resilience and efficiency are two sides of the same coin, the Fund has systematically integrated risk-informed decision-making into the very fabric of its digital transformation. This strategic alignment has not merely mitigated threats but has actively fueled a new standard of operational excellence, safeguarding member assets while drastically enhancing service delivery. The following case studies illustrate how a forward-looking risk posture has been instrumental in achieving transformative outcomes.

Case study 1: Automating high-risk payment process-massive automation

Challenge:

The manual batching of benefit payments represented a significant operational inefficiency. The repetitive nature of this process introduced systemic vulnerabilities, most critically, substantial delays in benefits payment turnaround times. These delays constituted a direct threat to the Fund's core mandate, exposing the organization to significant financial and reputational risk through its failure to ensure timely benefits disbursement.

The risk-informed strategic solution

The NSSF's response was not a mere automation exercise but a strategic deployment of Robotic Process Automation (RPA), engineered with an intrinsic risk control framework, to systematically eliminate the delays that plagued the manual process. By pre-empting failure points and embedding resilience, the solution moved beyond mere efficiency gains to ensure robust operational integrity and timely disbursements.

Key risk-mitigating features included:

Proactive alerting and immediate intervention

The system was built to provide instant, exception-based notifications, inclusive of any failed transaction batches, to the Benefits team members responsible. This control ensured that issues were contained and remediated in near real-time, transforming a previously reactive process into a proactive command-and-control function.

Built-in validation controls

To mitigate the risk of financial inaccuracies during benefits cleaning process, the RPA solution incorporates hard-coded validation rules. This eliminates the possibility of incorrect value selection and high-impact errors at the source, which were previously common.

Scalability and rigorous stress testing

Prior to deployment, the solution underwent exhaustive load testing in a controlled, non-production environment. This proactive measure validated system reliability and performance under peak transaction volumes, mitigating the significant operational and reputational risk of a system failure during critical payment cycles.

The results: Quantifiable gains in resilience and efficiency

This deliberate, risk-aware approach yielded measurable returns that extend far beyond simple time savings, fundamentally de-risking a critical operation.

i. **Drastically improved turnaround time**

   Benefit payment processing was accelerated to a record 5.6 days for FY 2024/2025, directly enhancing member satisfaction and trust.

ii. **Enhanced accuracy and integrity**

   The automation of repetitive tasks minimized human error, ensuring members received correct payments promptly and reducing the risk of financial discrepancies.

Strategic lesson learned

Integrating risk management into automation is not an impediment to speed; it is the essential prerequisite for achieving sustainable and secure operational efficiency. Proactive testing and continuous monitoring are not optional overheads but critical investments in long-term operational resilience.

Case Study 2: Intelligent process streamlining, leveraging data confidence as a risk mitigation tool

Challenge:

A one-size-fits-all claims process mandated that every submission undergoes a full manual review, irrespective of its inherent risk profile. This created a critical operational bottleneck, diverting staff to perform low-value verification on claims initiated with high data integrity. This inefficient allocation of resources increased processing times unnecessarily for low-risk member claims and created a drag on overall organizational agility.

The risk-informed strategic solution

The NSSF implemented an innovative "Automatic Skipping of Data Cleaning Stage" solution, which functions as an intelligent, data-driven risk filter. This approach moves from a static control environment to a dynamic one, where the control itself is conditional upon the assessed risk. The solution operates on a sophisticated framework

Quantifiable risk assessment

An Application Programing Interface (API) automatically analyzes each member's statement upon submission, assigning a quantifiable data cleanliness score. This score serves as a Key Risk Indicator (KRI).

Risk-appetite-aligned thresholding

The team established a stringent, risk-based threshold of 98.5% data cleanliness. Claims exceeding this benchmark are formally classified as low risk, aligning the process with the section's criteria for clean member statements.

Automated, conditional workflow bypass

Claims identified as low risk are automatically fast-tracked, bypassing the manual review by Contributions Manager. This creates a streamlined pathway for low-risk transactions while reserving manual scrutiny for higher-risk and complex cases.

The results:

i. **Reduced benefits payment cycle time, enhanced resource optimization and improved member experience**

Benefit payment processing was accelerated to 5.6 days in FY 2024/2025, from 10.12 days in the FY2023/2024, and resource allocation was optimized, while member experience greatly enhanced. Members with pristine data enjoy a frictionless and expedited claims process.

This targeted application of controls demonstrated that strategic risk-taking, when properly governed, is a catalyst for efficiency.

Staff are liberated from routine verification and redeployed to address complex, high-risk cases that genuinely require human judgment and intervention. This elevates the role of the officer from processor to problem-solver.

A faster, more intelligent process directly translates into a better member experience, building long-term trust and improving the Fund's reputation.

ii. **Enhanced transaction integrity**

The 98.5% threshold acts as a critical control gate, ensuring that only verifiably accurate claims are fast-tracked, thereby mitigating the risk of erroneous automatic approvals.

Strategic Lesson Learned

Effective risk management is the enabler of intelligent efficiency. By leveraging data quality as a dynamic risk indicator, organizations can move beyond rigid, uniform processes to create fluid, responsive operations. This demonstrates that an effective management of risk is not about risk avoidance, but about empowering strategic, member-centric innovation without compromising control.

Conclusion

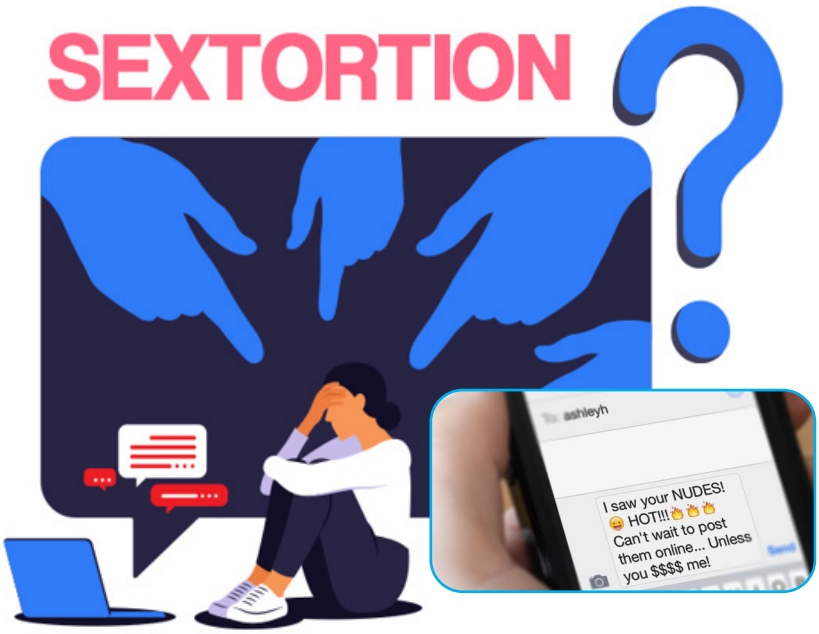
The NSSF's transformation journey underscores a critical paradigm shift that proactive risk management is no longer a defensive compliance function but a decisive strategic catalyst. By deliberately architecting risk mitigation into the core of its digital initiatives, the Fund has moved beyond merely guarding against threats to actively unlock new dimensions of value. The success in payment automation and process streamlining, demonstrates that a sophisticated and data-driven approach to risk does not hinder progress but it accelerates building a foundation of trust, resilience, and precision. ■

TEEN SEXTORTION & DEEPFAKES

A PARENT-COMMUNITY PLAYBOOK

Christine Hilda Namuddu
Information Security Manager & Data Protection Officer, NSSF

The digital revolution has opened extraordinary opportunities for learning, creativity, and connection. But it has also introduced new and unsettling risks - particularly for our teenagers. Among the most concerning of these are sextortion and deepfakes - two intertwined threats that exploit technology and psychology to manipulate, extort, and harm young people.



In Uganda, where smartphone penetration among youth is rising rapidly and mobile money usage is part of everyday life, the risks are real and immediate. Parents and educators need to act now, not later, to protect teenagers from falling victim to this new form of digital exploitation.

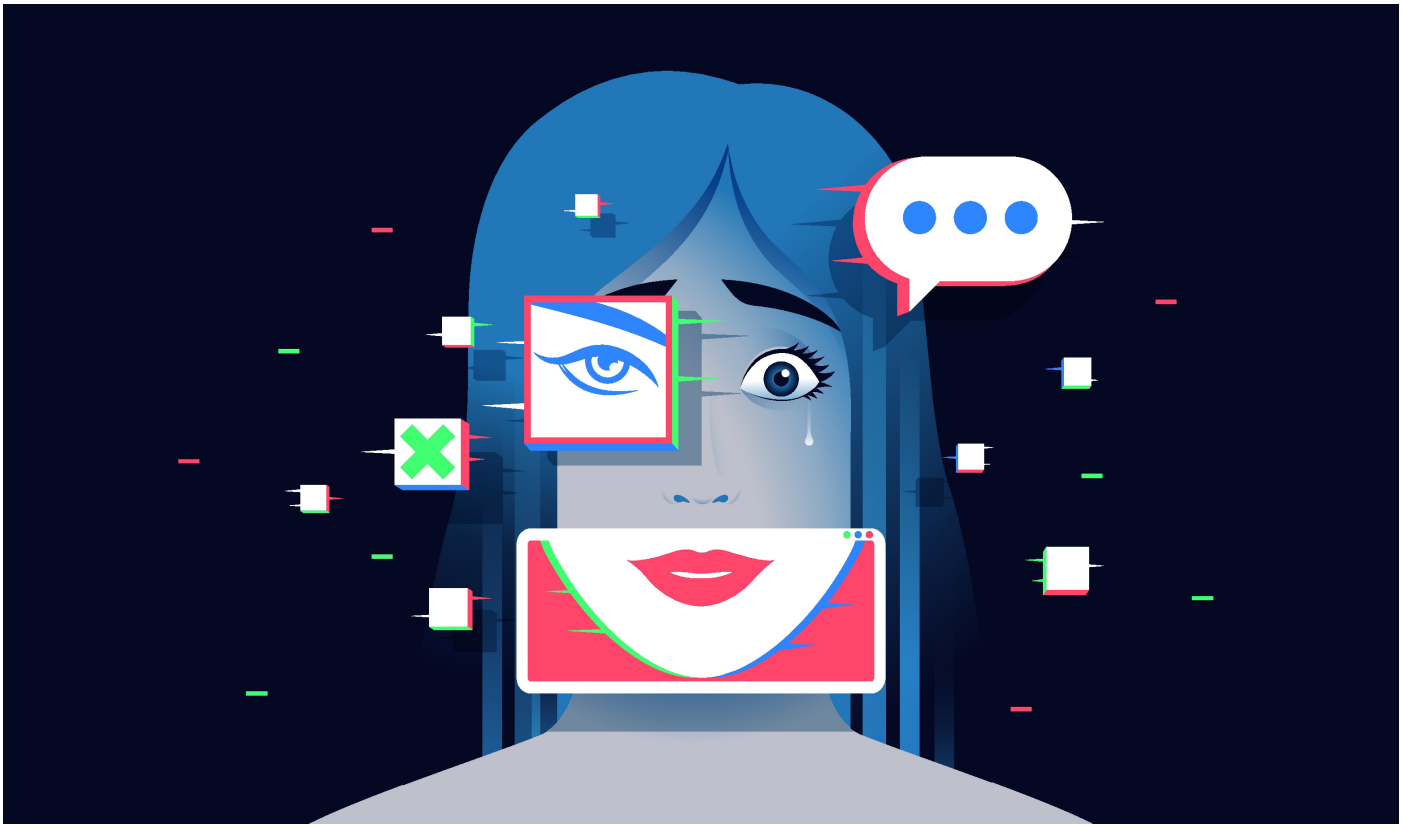
Understanding the threat

Sextortion is a form of online exploitation where perpetrators blackmail victims by threatening to release the victim's sexual images or videos unless demands are met. Demands often include money, more explicit content, or favors.

For teens, sextortion often begins innocently, for example, a new friend on Instagram asks for a photo; a gaming friend sends a flirty message, or a classmate pressures them over WhatsApp. Once a single compromising image is shared, the trap is set. The attacker then demands more pictures or money.

Jordan DeMay's case (Michigan, 2022-2023) illustrates the classic pattern of scammers posing as a peer coaxing for an explicit image, then demanding payment. Jordan, a 17-year-old high school athlete from Marquette, Michigan, was targeted by scammer posing as a teenage girl on Instagram. He shared intimate images and money was extorted from him after threats of sending the compromising photos to his friend and family. Jordan committed suicide just hours after the digital entrapment began.

Murray Dowey's case (Scotland, 2024) involved scammers on Instagram who coaxed an explicit image from the 16-year-old, then demanded money. Tragically, Murray committed suicide just hours after the extortion began. His case is particularly poignant because his family was well-informed



of the dangers and had discussed online safety, proving that even vigilant families can be targeted.

According to The Accra Times newspaper, Ghana's Cyber Security Authority recorded 141 sextortion complaints between March–June 2024, with financial losses amounting to GHC 112,209. In early 2025, financial losses quintupled, and victims lost GHC 500,000 in just four months.

The security awareness group KnowBe4 Africa issued an alert in September 2024 pointing to a growing number of sextortion attempts against teenage boys in South Africa. Criminals prey on social media, promising romantic interest before leveraging explicit content for extortion.

As smartphone use and digital literacy rise in Uganda, the entry points for sextortion are disturbingly familiar. Like a new friend on Instagram asks for a photo; a "gaming buddy" initiating a flirtatious chat; and a classmate pressuring through WhatsApp, among others.

Deepfakes: A dangerous shift

Deepfakes are artificially generated images, audio, or video created using AI. They can convincingly place someone's face onto another person's body or manipulate voice recordings.

For teens, deepfakes create two major risks: first, the creation of false images and videos where an innocent photo, like one from a school event, can be misused to generate fabricated and harmful sexual content; and second, voice manipulation, where audio clips from platforms like TikTok or class presentations can be exploited to produce deceptive and damaging fake recordings.

Deepfakes make sextortion even more dangerous because perpetrators do not even need a real photo as they can manufacture one.

In the case of Elijah "Eli" Heacock (Kentucky, USA, 2023), Elijah, 16, was sent an AI-generated deepfake nude of himself along with sextortion demands despite having no such photo in the first place. The attacker demanded US $3,000. Though he may have sent some money, he was unable to meet the demand. Subsequently, Elijah took his own life. This case highlights the terrifying reality that deep-fakes can be used to fabricate images, eliminating even the need for a real compromising photo.

Why Teens Are Targeted

Teens are disproportionately targeted because they are often trusting by nature and still developing a full sense of risk awareness, which is compounded by intense peer pressure and a fear of social exclusion that makes them vulnerable to coercion. Furthermore, their high digital presence, spending hours daily on platforms like WhatsApp, TikTok, Instagram, and online games, creates a vast attack surface for predators, who can also exploit them for financial gain through small but consequential mobile money transactions. Many teens operate without adequate guidance as their parents frequently possess less digital literacy than they do.

Warning Signs for Parents and Communities

Parents and communities should be vigilant for key behavioral indicators that a teen may be targeted, including sudden withdrawal from friends and previously enjoyed activities, unusual secrecy surrounding their devices and online interactions, visible anxiety or distress immediately after checking messages or notifications, and unexplained or urgent requests for money without a clear and legitimate reason.

Other key digital warning signs include the emergence of new, suspicious social media accounts with a minimal number of followers, excessive engagement in private messaging with unknown or unverified contacts and the frequent and deliberate deletion of chat histories to conceal interactions.

Preventive Cyber Hygiene for Families

Device Setup for Teenagers: A critical foundation for preventive cyber hygiene begins with the secure setup of a teenager's device, which includes enabling robust parental controls and content filters.

Family Rules for Digital Safety: To foster a culture of digital safety, families should establish clear rules that prohibit sharing personal photos with online-only friends and never disclose sensitive information like school IDs, National Identification Numbers (NINs), or home addresses. These rules should be reinforced through regular family "digital check-ins" to create an open and ongoing dialogue about online experiences.

Teaching Critical Thinking: Teaching critical thinking is essential and involves explaining to teens that not everything they encounter online is real, proactively showing them concrete examples of fake accounts and manipulated photos to build their discernment, and consistently encouraging them to develop a habit of pausing to critically evaluate content before posting anything themselves.

Managing Social Media Footprints: To significantly enhance privacy and security, it is crucial to set all social media profiles to the strictest private settings e.g, limit tagging permissions to prevent unwanted exposure, regularly reviewing and curating friends, removing unknown followers, and actively discourage the oversharing of personal moments that could be misused.

The Community's Role

Communities, including schools, families, and local organizations, are uniquely positioned to protect teens from sextortion by fostering awareness and embedding cyber hygiene into the culture of daily life.

Policy and Governance

In Uganda, teen sextortion in schools and homes has emerged as a pervasive threat, often manifesting as abuse of power intertwined with sexual exploitation. According to a 2025 parliamentary report, the Development Network of Indigenous Associations (DENIVA) advocated for the criminalization of sextortion under the Sexual Offences Bill, 2024, highlighting cases where perpetrators threaten to publish intimate images or videos to extort money or favors, including from vulnerable teens. These efforts should be supported.

Local communities should implement policies that are essential to combating sextortion, including Acceptable Use Policy (AUP), encouraging teens and parents to commit to safe digital practices

Program Integration

To build a comprehensive defense, communities must integrate digital citizenship into their programs through community-led workshops addressing modern threats like online safety, deepfakes, and sextortion. These should be supplemented by peer-to-peer mentorship initiatives, where teens learn digital resilience from one another, fostering a supportive environment to navigate online risks.

Community Infrastructure

A secure community infrastructure is vital to minimize sextortion risks. Communities with public internet spaces like schools, should provide protected Wi-Fi networks in public spaces with robust logging and content filtering to monitor and restrict harmful content. Offering community-managed

digital platforms for communication and activities reduces reliance on risky external tools. Additionally, comprehensive training for community leaders, including educators and local organizers, equips them to recognize and respond to early signs of online exploitation.

Crisis Management Planning

A well-defined crisis management plan is critical for addressing sextortion incidents. Communities must establish confidential and accessible reporting mechanisms for teens to report concerns safely. Clear response steps should be activated immediately upon suspicion of sextortion or other online exploitation, with a defined escalation path from community counselors or trusted leaders to law enforcement, ensuring a swift, coordinated response.

Responding to Sextortion or Deepfake Incidents

Stay calm and supportive: In the event of an incident, it is paramount for parents and caregivers to stay calm and supportive, remembering that the worst possible mistake is to blame the teenager, as they are the victims of exploitation and not the culprits of a crime.

Preserve evidence: It is critical to immediately preserve all available evidence by taking clear screenshots of conversations and profiles, saving all original messages, and meticulously recording any relevant transaction IDs, as this documentation is essential for reporting the crime and aiding any subsequent investigation.

Stop communication: It is imperative to immediately stop all communication with the perpetrator, and under no circumstances should you negotiate with them or pay any further money, as this only fuels their demands and prolongs the exploitation.

Report Incident: It is critical to immediately and comprehensively report the incident to all relevant authorities, which includes informing school authorities if the exploitation is linked to classmates, filing a formal report with the Uganda Police Force's Cyber Crimes Division for a criminal investigation, notifying the Uganda Communications Commission (UCC) to address any related telecom or mobile money abuse, and reporting the account and content to the specific platform (such as Facebook, Instagram, or TikTok) to request its immediate takedown.

Block and secure accounts: To immediately secure the victim's digital presence, it is essential to block the perpetrator on all platforms, change all account passwords to strong and unique alternatives, enable two-factor authentication (2FA) on every possible account to prevent unauthorized access, and meticulously disconnect any third-party accounts or apps that may have been linked, as these can be a continued source of vulnerability.

Psychological support: Providing immediate access to professional counseling services is essential for the victim's recovery, and this support must actively engage parents and guardians in the healing process to ensure a compassionate, unified, and effective response.

Legal Pathways: In pursuing justice, victims and their families should be made aware that Uganda's Computer Misuse Act and the Data Protection and Privacy Act provide critical legal avenues for recourse, offering a framework to hold perpetrators of cybercrimes and data exploitation accountable.

Building a Culture of Digital Resilience

Protecting teens in the digital age transcends technology and requires a fundamental shift in community mindset. For parents, this means normalizing open and ongoing conversations about online risks with the same urgency and regularity as discussions about road safety; for communities, it demands treating comprehensive cyber hygiene not as an optional lesson but as an essential, non-negotiable life skill integrated into the core curriculum; and for the wider community, it involves leveraging trusted local institutions like churches, youth groups, and NGOs to collectively spread awareness and create a unified culture of vigilance and support.

Conclusion

Sextortion and deepfakes may seem like global problems, but they are already here in Uganda. Our children are at risk - not because they are careless, but because they are growing up in a digital landscape where trust is exploited and technology is weaponized.

Parents and communities must stand together as the first line of defense. Through open conversations, strong digital hygiene practices, supportive policies, and proactive crisis response, we can create an environment where our teenagers are not just protected but empowered to thrive online. The threats are real, but with the right playbook, we can outsmart them. ■

> **And you, fathers, do not provoke your children to wrath, but bring them up in the training and admonition of the Lord.**
>
> Ephesians 6:4

Smartlife Flexi®

a better way to save

Everyone has a goal, what's yours?

Sign up for the **Smart**life **Flexi** plan via the **NSSFGo App/Web** or visit a branch near you. Visit **www.nssfug.org/smartlifeflexi** or call **0800 286 773** for details.

Save for **short & medium-term** goals	Easily **top up and track** your savings	Start with as low as **Shs 5,000**	***Access your savings** any time	Enjoy ***competitive returns**

Download the **NSSFGo App.** GET IT ON Google Play Download on the App Store

*Terms and conditions apply.

Making lives better.

NSSF a better life | 40 Years Making Lives Better

AI THE DOUBLE-EDGED SWORD

Andrew Kapere
Information Security & Compliance Manager,
Deposit Protection Fund

It is strategically necessary for businesses to incorporate Artificial Intelligence (AI) into their operations. According to McKinsey's "The state of AI in 2025" global survey, 88% of organizations reported regular use of AI, with 92.1% of these noting positive results including improved levels of accuracy, efficiency, growth and cost savings. However, despite the great benefits associated with AI, the implementation of AI poses a substantial and complex risk portfolio for HR management, which needs to be actively managed. Navigating the organizational and human risks that technology introduces is the true test of leadership, not the technology itself.

The efficiency gain:

The business case for AI is robust, driven by benefits including:

- **Hyper-automation of routine tasks:** By performing repetitive, high-volume tasks flawlessly and lowering errors in data entry, scheduling, compliance checks, among others, AI lowers operational risk
- **Improved data-driven decision making:** AI algorithms analyze vast datasets to find patterns and forecast trends, reducing strategic risk through improved inventory control, targeted advertising, predictive maintenance, etc.
- **24/7 operational capacity:** AI systems guarantee business continuity, reducing operational risk related to human fatigue and limited capacity for worldwide customer support and monitoring.
- **Reduction in human error:** AI's accuracy reduced financial risk and compliance in tasks like financial reconciliation, shielding companies from fine.

From a purely operational standpoint, AI is a powerful tool for risk mitigation and value creation. However, it simultaneously introduces a new set of human-centric risks that, if left unmanaged, can negate these very benefits.

The human impact: Identifying the hidden risk factors

The ability of AI to handle routine or repetitive tasks with the highest degree of accuracy and speed, presents critical risks that fall directly within human resource management (HRM)'s purview.

1. **Talent and cultural risk:** The most immediate danger is the anxiety and fear surrounding

McKinsey's "The state of AI in 2025" global survey

88%

Percentage of organizations using AI regularly

92.1%

Percentage of organization that noted positive results

job displacement. This poses a severe cultural risk, undermining psychological safety, morale, and trust. A culture of fear leads to resistance, silence, and attrition, destroying the collaborative environment necessary for innovation.

2. **Skills gap and operational risk:** Failing to future-proof your workforce creates a profound strategic and operational risk. If AI handles all analytical tasks and the organization hasn't reskilled its employees, it creates a critical skills deficit. The company becomes unable to manage, interpret, or ethically oversee the very AI systems it depends on, leading to new vulnerabilities.

3. **Employee engagement and productivity risk:** When roles are reduced to merely overseeing AI, it leads to under-stimulation and deskilling. This productivity risk manifests as a drop in engagement, innovation, and critical thinking.

4. **Reputational and ethical risk:** How a company handles the AI transition will be scrutinized by remaining employees, the job market, and the public. Layoffs handled poorly, or a perception that the company values efficiency over people, constitutes a significant reputational risk, damaging employer branding and the ability to attract top talent in the future.

The AI Pivot's Human Impact: Cases of layoffs in cybersecurity firms

The cybersecurity sector is experiencing a wave of layoffs as companies reallocate resources toward artificial intelligence, a trend starkly illustrated by the case of Deepwatch.

In November 2025, the cybersecurity firm Deepwatch, laid off between 60 and 80 employees, a cut that impacted nearly a third of its roughly 250-person workforce. The company's CEO, John DiLullo, stated the move was to align the organization and "….accelerate our significant investments in AI and automation".

Deepwatch is not an isolated case, they join other cybersecurity companies like CrowdStrike, Deep Instinct, and Sophos, which have also conducted layoffs in 2025.

This trend raises a crucial question for HR management: Are these layoffs a genuine transformation of the workforce or a form of "AI-washing"?

Embedding risk management into the Human-AI strategy

HRM must evolve from a support function to a core risk management partner. The response must be strategic, proactive, and integrated.

Mitigate talent risk with transparent communication: Reframe the narrative from replacement to augmentation. Proactively communicate that AI is a tool to eliminate tedious work, mitigating cultural risk by reducing fear and building trust. Transparent roadmaps about the future of work within the organization are crucial.

Treat reskilling as risk mitigation: Investing in transitional support is not an employee benefit; it is a direct strategy to mitigate strategic risk.

- **Conduct skills gap audits:** Identify current capabilities and future needs to understand the scale of the risk.
- **Create reskilling pathways:** Develop partnerships with learning institutions to offer certifications in data literacy, AI management etc. This builds a resilient, future-proof workforce.
- **Offer career transition counseling:** For roles that will be phased out, supportive outplacement or internal mobility programs mitigate reputational risk and demonstrate a commitment to ethical stewardship.

Redesign roles to mitigate productivity risk: Redesign jobs for human-AI collaboration. This ensures employees engage in higher-value work, protecting against the risk of disengagement and preserving crucial human judgment in the loop.

Implement ethical governance to manage compliance risk: HRM must partner with legal and IT departments to establish guidelines for ethical AI use. This includes auditing algorithms for bias (mitigating compliance and reputational risk), ensuring data privacy, and creating clear accountability structures for AI-driven decisions.

Champion continuous feedback as an early-warning system: Create formal channels for employee feedback on AI tools and the transition process. This serves as an early-warning risk detection system, identifying cultural friction, usability issues, and training gaps before they escalate into larger crises.

Conclusion

The application of AI in business operations is real, but its introduction is high stakes change management initiative. The ultimate success of AI will be measured not just by its efficiency gains, but by an organization's ability to emerge from the transition more agile, innovative, and human-centric than before. The goal is to be a resilient organization where technology and people thrive in a carefully managed balance. ■

DIGITAL FORENSICS

A STRATEGIC TOOL FOR MANAGING CYBER RISK

Phiona Taaka,
Incident Handling and Forensics, UCC

In today's interconnected world, cyber threats are no longer a rare disruption; they are constant realities. From ransomware that locks down entire networks to insider misuse of sensitive data, a single incident can halt operations, erode customer trust, and inflict lasting financial damage.

As organizations increasingly depend on digital assets to run their businesses, the ability to detect, investigate, and respond to cyber incidents has become critical. This is where digital forensics steps in, not just as a tool for solving crimes after they occur, but as a vital component of modern risk management.

Key Cyber Threats and Their Risk Implications

Organizations face a growing range of cyber threats that can significantly disrupt operations, erode stakeholder trust, and result in financial and reputational damage. From a risk management perspective, understanding these threats is essential for effective mitigation and resilience planning. Key threats include:

Data Breaches

Unauthorized access to sensitive or confidential information, whether due to external attacks or internal mishandling, can lead to regulatory penalties, legal liabilities, and loss of customer trust.

Ransomware Attacks

Cybercriminals sometimes lock access to important company systems and files, and demand payment to unlock them. These attacks can halt operations, cause significant recovery costs, and damage brand reputation. Business continuity planning and regular data backups are essential risk mitigation strategies.

Phishing and Social Engineering

Deceptive tactics such as fraudulent emails or impersonation are used to trick employees into revealing credentials or initiating unauthorized transactions. These threat actors exploit human vulnerabilities, making security awareness training and multi-factor authentication vital components of a risk-aware culture.

Insider Threats

Risks posed by employees, contractors, or partners, whether through negligence or malicious intent, can lead to data leaks, fraud, or sabotage. Implementing strict access controls, monitoring, and fostering a culture of accountability are key to managing insider risks.

The Role of Digital Forensics in Investigations

Digital forensics involves examining electronic devices like computers, phones, USB drives, and network equipment to uncover evidence that can help in investigations. This evidence can support decisions made by company leadership or be used in legal cases.

A key part of digital forensics is maintaining a chain of custody. This means carefully tracking and protecting evidence from the moment it's collected until it is used in court or presented to management. It helps ensure that the evidence is trustworthy and has not been tampered with.

In the corporate world, digital forensics is useful for identifying who was behind cyber incidents such as malware attacks, data leaks, or system disruptions. It's also used by law enforcement to investigate serious crimes. For example, in Uganda, the Uganda Revenue Authority has used forensic techniques to catch tax evaders.

Common Techniques in Digital Forensics

Data Recovery: This involves retrieving files that were deleted or damaged, whether accidentally or during a cyberattack. It helps restore important information and supports business continuity.

Network Forensics: By examining internet and network activity, investigators can trace how attackers got in and what they did. This is crucial for identifying weak points and improving defenses.

Mobile Forensics: With smartphones and tablets now central to work, this technique focuses on safely extracting data from mobile devices to uncover evidence or misuse.

File System Analysis: This helps investigators understand how files were accessed or modified, offering insights into user behavior and potential misuse of systems.

Strengthening Risk Management Through Forensics

Digital forensics plays a vital role in helping organizations not only respond to incidents but also strengthen their overall risk posture.

Here's how forensic investigations support effective risk managemen:

1. Understanding What Went Wrong

After a cyber-incident, digital forensics helps uncover how it happened. By examining digital evidence, organizations can trace the root cause, whether it was a system flaw, human error, or malicious activity. This allows for more targeted fixes that address the real problem, not just the symptoms.

2. Supporting Accountability and Compliance

Forensic evidence can be used to report incidents to regulators, support legal action, or cooperate with law enforcement. This ensures that organizations can respond transparently and meet their obligations under data protection and cybersecurity laws.

3. Turning Lessons into Safeguards

Every incident offers valuable lessons. Forensics provides insights that help organizations improve their defenses, whether by updating policies, enhancing employee training, or tightening technical controls. In this way, past breaches become steppingstones for a more secure future.

Conclusion

Digital forensics is no longer just a reactive tool but a strategic asset in risk management. By integrating forensic capabilities into incident response plans, organizations can move from damage control to proactive defense. Evidence from investigations enables stakeholders to make informed decisions and strengthens legal cases when needed. In a world where cyber threats are inevitable, having skilled forensic experts isn't optional but essential. ■

THE RISE OF AI AND ITS RISK IMPLICATIONS

A PERSPECTIVE FROM INFORMATION SECURITY

Arnold Mwesigwa
Information Security Specialist, NSSF

Artificial Intelligence (AI) is currently revolutionizing workplaces worldwide. From boosting productivity to sparking innovation, AI is becoming central to everyday business operations. Tools such as ChatGPT, Copilot, Grok, intelligent chatbots, and automated decision-making systems help organizations to streamline workflows, respond to customer needs faster, and analyze vast volumes of data at remarkable speed.

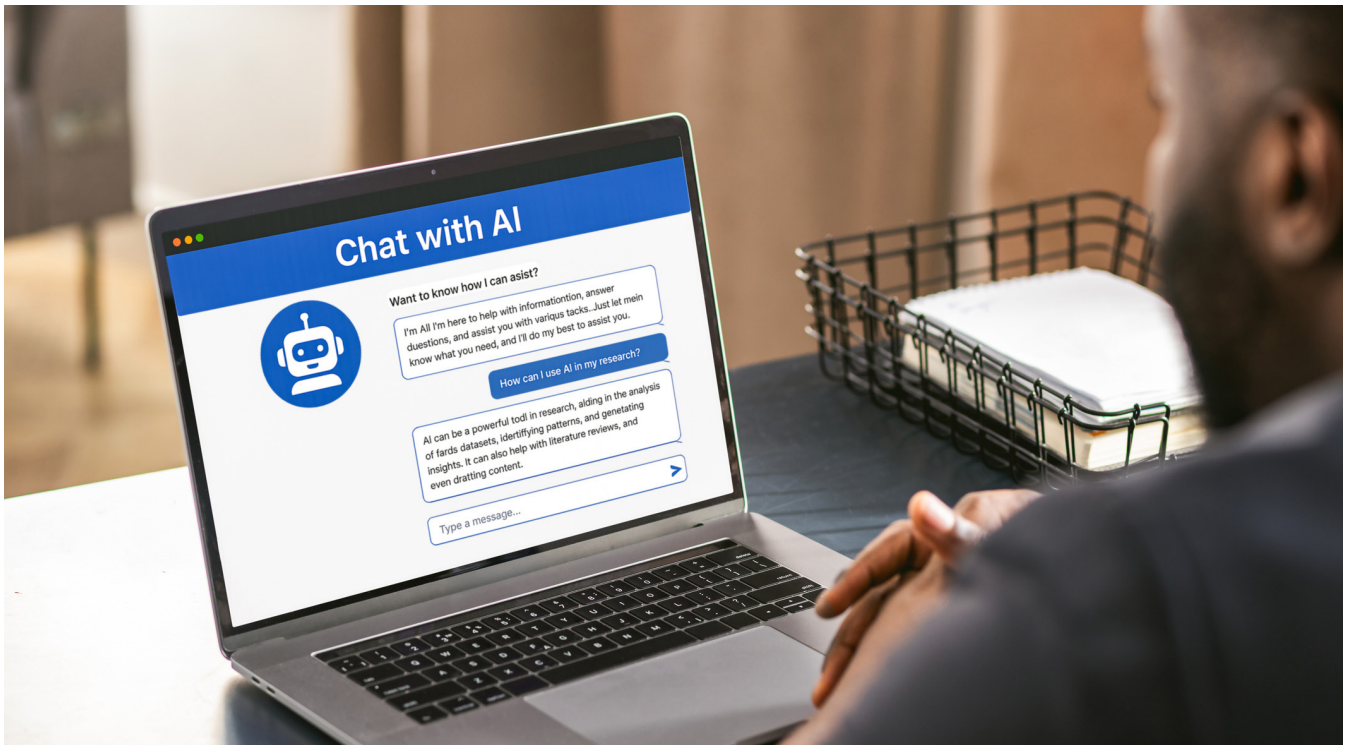
While AI's benefits are undeniably great, its integration into core business functions also raises important questions about information security, data privacy, and organizational risk. This article examines both the opportunities AI creates for enterprise risk management and the unique challenges it introduces to the information security landscape. By understanding this balance, we can prepare better for a future where AI plays a central role in business operations.

The Promise of AI in the Enterprise

AI is delivering substantial value across various business domains. In the enterprise context, it accelerates productivity, enhances decision-making, and improves customer engagement. An immediate advantage of AI is its ability to automate repetitive and time-consuming tasks, allowing employees to focus on more strategic, high-value activities. This improves operational efficiency.

Beyond automation, AI's capability to analyze massive datasets enables organizations to identify patterns and insights that would otherwise go unnoticed. Whether it's identifying emerging market trends, optimizing supply chains, or forecasting customer behavior, AI-powered analytics provide a strong foundation for informed decision-making.

Moreover, AI is becoming a vital ally in risk detection and fraud prevention. Machine learning algorithms can analyze transactional data in real time to detect anomalies and flag



potentially fraudulent activities. These capabilities are not only improving security but also reducing financial and reputational losses for organizations.

By enhancing data visibility, predicting potential threats, and supporting proactive decision-making, AI helps organizations navigate complexity and uncertainty more effectively. When integrated thoughtfully, AI becomes a key enabler of resilience and long-term business success.

AI Risks and Security Concerns

While AI's benefits are immense, its implications for data protection, compliance, and threat landscapes cannot be ignored. Below are some of the key risks organizations must be prepared to address.

a) Data Privacy and Confidentiality

Many AI tools, especially those used for content generation, predictive analytics, and automation, require access to large volumes of data, much of which may be sensitive or confidential. This includes customer information, internal communications, financial records, and intellectual property.

The major risk lies in the potential for data leakage or unauthorized access. If AI systems are not properly secured, they can lead to unintentional data exposure or malicious exploitation. For example, AI models trained on sensitive datasets may inadvertently "memorize" and reveal confidential information in outputs. Additionally, if access controls are weak, internal misuse or external breaches become more likely.

Information security teams must ensure that data minimization, encryption, access management, and usage auditing are core components of AI deployments to protect privacy and confidentiality at all stages of the AI lifecycle.

b) Model Bias and Decision Integrity

AI systems are only as objective as the data they are trained on, and that data often reflects historical biases or incomplete perspectives. This creates a significant risk of biased decision-making, especially in high-stakes domains such as hiring, due diligence, or fraud detection.

Moreover, many AI models operate as "black boxes," with little transparency in how they generate outputs. This lack of visibility can undermine trust and accountability, making it difficult to explain or justify decisions to stakeholders, regulators, or affected individuals.

The consequences of biased or opaque AI decisions can include unfair treatment of customers, employees or other stakeholders, regulatory scrutiny, and reputational damage. To mitigate this, organizations must implement AI governance frameworks, perform regular bias audits, and ensure human oversight for critical decisions influenced by AI outputs.

c) Shadow AI and Unapproved Tools

The accessibility of generative AI and other cloud-based tools has led to a rise in "shadow AI", when employees use AI services without organizational approval or oversight. While these tools may boost productivity, they often bypass established security protocols, introducing significant risks.

> **Shadow AI tools often bypass established security protocols, introducing significant risks.**

Unapproved AI platforms may store or process sensitive enterprise data in unknown locations or with inadequate safeguards, leading to data residency violations, compliance breaches, or intellectual property disclosure. Additionally, they may not meet the organization's standards for privacy, encryption, or contractual protection.

To counter this, organizations should create clear policies on AI usage, increase employee awareness, and provide approved alternatives that are secure, compliant, and user-friendly.

d) AI-Driven Threats

AI is not only a tool for defenders; it is increasingly being weaponized by attackers. Malicious actors are now leveraging AI to conduct more sophisticated cyberattacks, including:

- Deep fakes used for impersonation or social engineering
- Automated phishing campaigns tailored to individual targets
- AI-powered malware that adapts in real time to evade detection

These developments raise the stakes for cybersecurity teams, who must now anticipate AI-enabled adversaries with faster, more convincing, and more scalable attack methods. Traditional security controls may no longer be sufficient in this environment.

Organizations should invest in AI-powered defenses, such as behavioral anomaly detection, and stay informed about emerging threat vectors to maintain a strong security posture in an AI-accelerated threat landscape.

Mitigating AI Risks through Governance

To harness the benefits of AI responsibly, organizations should adopt robust governance frameworks such as the NIST AI Risk Management Framework that align technological innovation with risk management and regulatory compliance. AI governance provides the structure needed to ensure that AI systems are secure, ethical, transparent, and aligned with business objectives.

Information security plays a central role in this governance. First, it must establish access controls that limit who can interact with AI tools and what data they can process. Role-based access, multi-factor authentication, and data classification policies are essential to ensure that sensitive information is not exposed or misused.

Secondly, information security teams must monitor AI usage across the organization. This includes tracking data flows, logging model activity, and identifying instances of shadow AI. Such visibility is critical for enforcing compliance and quickly detecting anomalies or policy violations.

Thirdly, AI systems must comply with applicable data protection regulations, such as Uganda's Data Protection and Privacy Act (2019). This requires organizations to obtain proper consent, maintain data accuracy, uphold data subject rights, and ensure secure cross-border data transfers. Failure to do so, not only risks penalties but can also erode customer trust.

Organizations should conduct risk assessments specific to AI tools, integrate AI risks into enterprise risk registers, and develop mitigation strategies that account for both technical and business implications. This unified approach ensures that AI initiatives are not only innovative but also resilient and compliant.

Building Awareness and a Risk-Conscious Culture

Technology alone cannot secure AI because people play a crucial role. Organizations must cultivate a culture where employees understand the risks associated with AI and feel empowered to use these tools responsibly.

A key step is to encourage staff to be mindful of how they interact with AI by informing them what data is appropriate to share, which tools are authorized, and when to escalate concerns about harmful or unethical AI behavior.

Training and awareness campaigns should be tailored to different roles and departments, highlighting real-world examples of AI misuse and best practices for safe usage. These programs should be continuous, keeping pace with rapid developments in AI technologies. Providing simple, actionable guidelines is equally important. For instance:

- Do not input sensitive or personal data into public AI tools.
- Use only organization-approved platforms.
- Verify AI-generated content before using it for decisions or communications.

When awareness is widespread and AI literacy is high, organizations can reduce unintentional risks and promote a more secure, informed approach to AI adoption.

Conclusion

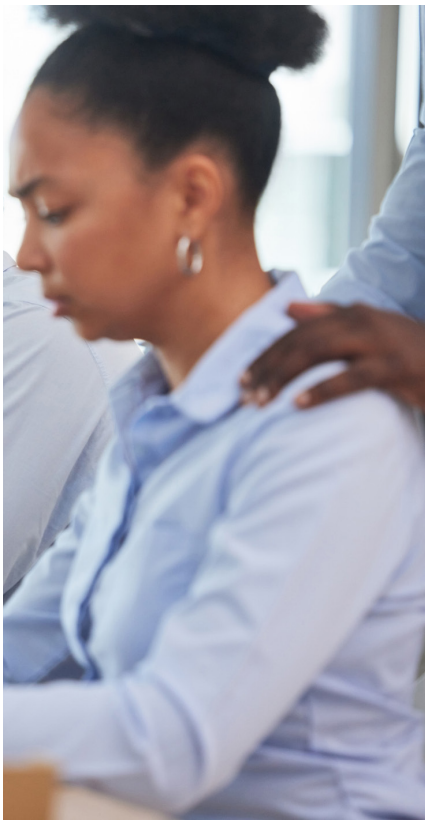
AI offers powerful capabilities that can enhance efficiency, drive innovation, and improve risk management. However, it also introduces new vulnerabilities, ranging from data privacy concerns to sophisticated cyber threats that must not be overlooked.

To navigate the dual nature of AI, organizations must take a proactive approach to risk management, embedding governance, security, and ethical considerations into every stage of AI adoption. This effort requires cross-functional collaboration among information security, enterprise risk management, legal, and operational teams to ensure AI is both beneficial and secure. ■

COMBATING SEXUAL EXPLOITATION, ABUSE AND HARASSMENT (SEAH) IN CORPORATE ENTITIES

Brian Mukalazi
CEO, Talis Consults Ltd

For individuals and entities working in the NGO sector, the terms Sexual Exploitation, Abuse, and Harassment - commonly abbreviated as SEAH - are familiar. This is unsurprising, given the sector's work with children, families, and communities in vulnerable settings, who are highly susceptible to these threats.



Over the years, numerous SEAH cases have been reported, often involving staff or partners of NGOs and Civil Society Organizations (CSOs), abusing the very beneficiaries they are tasked with protecting. Some cases have brought entire organizations to the brink of collapse. A prominent example is SOS Children's Villages, one of the world's largest child-focused NGOs. In 2021, the organization faced serious allegations of sexual abuse, exploitation, and systemic organizational failures spanning decades.

Investigations revealed a culture where evidence was destroyed, complaints were silenced, and staff who raised concerns were punished. There were also reports of donors and outsiders being granted inappropriate access to children, leading to further exploitation. These abuses were documented across multiple continents, with cases going as far back as the 1980s and 1990s in countries such as Nepal and Panama.

In response, SOS Children's Villages launched a Safeguarding Action Plan in 2021 and empowered an Independent Special Commission (ISC) to investigate these past failures. By 2023, the ISC confirmed sexual and physical abuse, forced abortions, cover-ups, and corruption. Some survivors had endured intimidation or expulsion when attempting to report.

Since then, the Organization has issued public apologies, established a global ombudsperson system, revised safeguarding policies, and provided tailored support to over 500 victims. Yet, despite these efforts, much of the damage - both organizational and personal - remains irreversible.

While SEAH is often associated with the NGO sector, corporate entities are not immune. Financial institutions, professional service firms, insurance companies, government agencies and other corporate bodies may not have program beneficiaries, but they do have employees, clients, and partners who are vulnerable to exploitation, abuse, or harassment.

Having worked across both corporate and NGO settings, I have observed that SEAH is often underprioritized in corporate environments - a gap that must be addressed.

Understanding SEAH

To address SEAH effectively, corporate leaders and employees must first understand what it entails:

Sexual exploitation involves taking advantage of another person's vulnerability or a position of trust for sexual purposes, often in exchange for money, gifts, or favors. It arises from misused power or dependency for sexual gain.

Sexual abuse is any unwanted sexual activity forced on a person without consent, including molestation, assault, or coercion. It often involves misuse of authority or manipulation.

Sexual harassment is unwanted sexual behavior - verbal, non-verbal, or physical - that creates a hostile or offensive environment, including inappropriate comments, gestures, sexual advances, or requests for sexual favors.

Research indicates that approximately one in four subjects of SEAH allegations occupy senior management positions *(CHS Alliance, 2023)*, underscoring the importance of accountability at every level of an organization.

Reporting SEAH Cases

Every employee has a responsibility to report SEAH, but reporting remains alarmingly low in many corporate environments. The problem is many staff are unaware of the applicable laws, regulations, and internal policies, leading to uncertainty about how to act when they witness or suspect misconduct.

The problem is further exacerbated by the lack of safe, accessible reporting mechanisms. Victims often face barriers, including fear of retaliation and lack of trust in management or investigative systems. Women, who comprise the majority of SEAH survivors, are disproportionately affected and often left isolated and unsupported.

Creating an environment that encourages and protects reporting is, therefore, essential. Entities must invest in awareness campaigns, staff training, and confidential reporting channels that empower victims and bystanders to come forward without fear.

Conducting SEAH Investigations

In many corporate entities, SEAH complaints are either not investigated or are handled poorly, preventing appropriate follow-up actions.

Formal investigations should be sanctioned whenever there is a credible allegation of SEAH. Entities must implement proper protocols that adhere to established investigative principles, including the following:

Figure 1

A high-quality investigation generally follows a structured process as highlighted in ***Figure 2.***

Figure 3 shows how one can ensure that they are conducting a Quality Investigation.

Disciplinary Procedures and Sanctioning

Once an investigation is completed, disciplinary procedures must be conducted fairly and transparently. Common pitfalls in many entities include bias, collusion, and negligence, which often invalidate proceedings.

Corporate entities must ensure that disciplinary proceedings comply with fundamental principles of fairness, justice, and transparency, as outlined in laws such as the Uganda Employment Act 2006. Key practices include:

- Providing notice of allegations to the employee (Subject of Allegation, SOA) with sufficient time to prepare a defense.
- Clearly stating the allegations and rights of the SOA during the hearing.
- Instituting an impartial disciplinary committee competent to hear the grievance.
- Providing anonymized investigation findings to the SOA in advance.
- Ensuring disciplinary decisions and sanctions are appropriate and proportionate.
- Clearly communicating the appeal process.

Failure to adhere to these principles can result in cases being contested in labor offices or the industrial court, with many entities losing due to procedural lapses.

Taking Action: A Message to Corporate Leaders

As a Corporate leader, you have a pivotal role in creating a safe workplace where Sexual Exploitation, Abuse, and Harassment (SEAH) is neither tolerated nor ignored. This is not just about compliance - it is about shaping culture, protecting people, and safeguarding your organization's reputation.

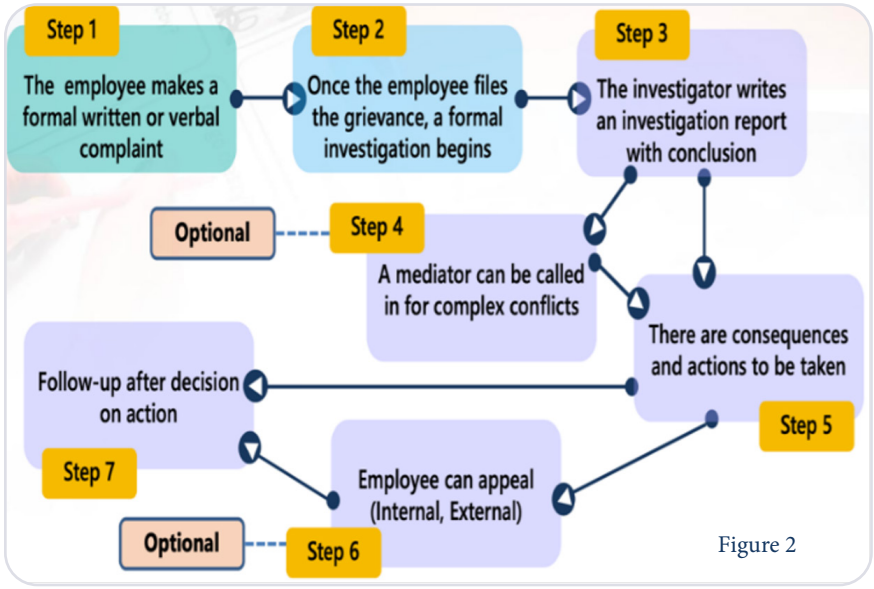


Figure 2

Figure 3

Start by designing and enforcing clear policies that leave no ambiguity about acceptable behavior and consequences for violations. Policies alone are not enough; you must train your staff consistently so that everyone understands SEAH, knows how to report it, and feels empowered to act.

Mitigate the risk by implementing safe recruitment practices, conducting thorough background checks, and establishing structured onboarding. Appoint dedicated safeguarding focal points to provide guidance and ensure employees have trusted channels to raise concerns.

Regularly monitor and evaluate policies, risk measures, and incident reports to ensure effectiveness. But the most powerful change comes from culture: lead by example, champion accountability and transparency, reward ethical behavior, and discourage silence or complicity.

You are the first line of defense. The actions you take - visible, consistent, and unwavering - send a clear message: SEAH will not be ignored. Protect your employees, your clients, and the integrity of your entities by making safety, trust, and accountability non-negotiable. ■

NOT ALL THAT GLITTERS IS GOLD

Andrew Mwima
Financial Advisor

Credit: Investopedia / NoNo Flores

During a guest-speaking engagement in a church on financial stewardship, I shared practical insights on personal finance - budgeting, documenting financial plans, investing, and preparing for retirement. When discussing investments, I highlighted historical average returns from conventional markets like stocks, bonds, and unit trusts, which typically range from 15% to 25% annually. In the front pew, Jacob listened intently, his curiosity palpable.

After the service, Jacob approached me, visibly disappointed with the returns I had mentioned. He urged me to attend a presentation in town, promising I'd learn about an opportunity offering up to 50% monthly returns. Intrigued, I agreed to join him.

The event took place in a polished, well-furnished building, buzzing with excitement. Jacob introduced me to several relatives- aunts, uncles, and siblings whom he had recruited into this "high-return" venture. A charismatic presenter soon took the stage, displaying a spreadsheet detailing monthly payouts for investments ranging from UGX 2 million to 100 million. The room's enthusiasm peaked when a trader boldly pledged UGX 500 million.

However, as the presentation unfolded, red flags emerged: promises of unrealistic returns, vague explanations, and an overly enthusiastic pitch lacking substance. I quietly warned Jacob that something seemed off. Tragically, my concerns were validated months later when Jacob and his group fell victim to a ponzi scheme, losing significant sums of money.

Identifying Ponzi Schemes: Key Warning Signs

A ponzi scheme is a fraudulent investment scam where returns for earlier investors are paid using funds from newer investors, not legitimate profits. To protect yourself, watch for these telltale signs:

1. **Unrealistically High Returns with Little or No Risk.**

   Promises of consistent above-market returns (e.g., "15% monthly guaranteed") are a major warning sign. Legitimate investments carry risks, and high returns with zero risk don't exist.

Conduct thorough research to avoid losing money to Ponzi Schemes.

2. **Lack of Transparency.**

   If the company avoids explaining how profits are generated or uses vague, complex jargon, be cautious. Legitimate businesses allow you to verify their business model or assets independently.

3. **Unregistered Investments or Advisors.**

   Ponzi schemes often operate without licenses from financial regulators, such as Uganda's Capital Markets Authority or Bank of Uganda (BOU). Always verify registration with relevant authorities.

4. **Reliance on Recruiting New Investors.**

   If you're encouraged or rewarded for recruiting others, it's a red flag. Legitimate investments focus on assets or business performance, not recruitment.

5. **Difficulty In Withdrawing Funds.**

   Delays, excuses, or restrictions when withdrawing money signal trouble. Ponzi schemes often collapse when withdrawals outpace new investments.

6. **Unverifiable Account Statements.**

   Beware of fake or unverifiable online dashboards showing returns. Legitimate investments provide statements from independent, audited sources.

7. **Lifestyle and Marketing**

   Promoters flaunting wealth, luxury cars, or "success" stories, often through social media influencers or testimonials, prioritize hype over verified financial data.

How to Protect Yourself

To avoid falling prey to scams like ponzi schemes:

- Verify the company's registration with the relevant authorities.
- Ask detailed questions and walk away if answers are unclear or evasive.
- Consult an independent financial advisor before investing.
- Resist pressure to invest quickly or secretly.
- Conduct thorough research and prioritize regulated, transparent opportunities.

Conclusion

Jacob's story serves as a sobering reminder that not all that glitters is gold. The allure of quick, high returns can cloud judgment, but vigilance and due diligence are essential for financial security. By paying attention to warning signs of ponzi schemes and prioritize transparency and independent advice, you can protect your hard-earned money and build a stable financial future. Always approach opportunities which are too good to be true with caution, skepticism, and a commitment to informed decision-making. ■

> **Promises of consistent above-market returns are a major warning sign common with Ponzi Schemes**

THE RISK OF NOT PLANNING FOR YOUR LONG-TERM FUTURE

Aisha Nakanwagi
Financial Literacy Officer - Mass Personalization, NSSF

In Uganda, the pressing demands of daily life such as school fees, medical bills, and rising living costs grab the attention of many individuals and families. While these immediate needs are undeniably inevitable, neglecting long-term planning poses significant risks that can jeopardize one's future financial security and dignity.

A Story from the Classroom

During financial literacy workshops, I often pose a question to participants: "What phrase do you use to justify spending money without guilt?" The responses, often humorous, spark meaningful reflection.

Participants might exclaim, "YOLO – You Only Live Once!" or quip, "If the money you have can't solve your problems, eat it." These lighthearted remarks reveal a common mindset among Ugandans: money is primarily for addressing immediate needs or savoring the moment.

Morgan Housel, in The Psychology of Money, observes that people spend for two main reasons: to bring happiness to themselves and their loved ones or to impress others. These motivations often guide our financial choices, but the risk lies in making decisions without weighing their long-term consequences.

The Hidden Risk

Failing to plan for the future is itself a significant risk. Without savings, investments, or retirement plans, many Ugandans face the prospect of poverty in old age, dependence on their children, or the inability to afford healthcare and lifestyle needs later in life. According to the Uganda Retirement Benefits Regulatory Authority (URBRA), less than 15% of working Ugandans are enrolled in pension schemes, leaving the majority vulnerable in old age, when they can no longer earn an income.

Why It Happens- Not planning for the future

Several cultural and structural factors contribute to this planning gap.

a) Income Instability

Many Ugandans rely on informal or seasonal income sources, such as farming or small-scale trading, where earnings are irregular and often tied to factors like weather or harvests. For instance, tobacco farmers in Northern Uganda typically receive a single annual payout after a nine-month crop cycle. Without disciplined planning, this lump sum is often spent quickly, leaving families struggling until the next harvest.

b) Cultural Expectations

Historically, children were expected to support their aging parents. However, urban migration, smaller family sizes, and youth unemployment, have weakened this traditional safety net. Parents who rely solely on their children for survival may be hit by the harsh reality that their children are no longer providing any support.

c) Low Awareness

Many Ugandans believe retirement planning is only for those in formal employment. Few are aware that market vendors, artisans, or self-employed individuals can make voluntary contributions to the National Social Security Fund (NSSF), join Savings and Credit Cooperative Organizations (SACCOs), or participate in investment clubs. Limited access to clear, trustworthy information keeps people trapped in short-term survival mode.

Consequences of lack of long-term planning

The absence of long-term planning exposes individuals to several dangers.

a) Financial Shocks

A single medical emergency can erase years of hard work. For example, an uninsured rural family might sell land, livestock, or withdraw children from school to cover hospital bills.

b) Dependency

Elderly individuals without savings often rely on their children or extended family. In a country where many young people face unemployment or underemployment, this creates a cycle of financial strain across generations.

c) Missed Opportunities

Without planning, long-term goals like purchasing land, building a home, or educating children become elusive. Dreams give way to daily survival, and opportunities for wealth creation are lost.

The Safer Path Forward

Long-term planning is not just for the wealthy, it's for everyone. Small, consistent actions can yield significant results.

i) Join a Retirement Savings Scheme

Beyond mandatory contributions, salaried workers and self-employed individuals can make voluntary payments to NSSF or other licensed funds. Even a modest monthly contribution of ten thousand shillings can grow into a meaningful safety net over time.

ii) Participate in SACCOs or Village Savings Groups with Discipline

Many Ugandans belong to savings groups but often withdraw funds for short-term needs like weddings or funerals. By setting rules to preserve a portion of savings for investment, SACCOs can become powerful tools for wealth-building.

iii) Teach Children Financial Discipline

Breaking the cycle of poor financial planning starts with the young. Teaching children to manage money fosters lifelong habits. In a recent pilot program in Northern Uganda, NSSF introduced financial literacy sessions in schools. Students formed savings clubs, contributing small amounts of pocket money weekly and setting collective goals. At the end of the term, they used their savings for meaningful projects, such as buying school supplies or starting small gardens.

The impact was striking not in the amount saved, but in the shift in mindset. Children who once spent pocket money on sweets began discussing budgeting, investment, and prioritizing needs over wants. Teachers noted that parents observed changes at home, with children encouraging saving for the future. By equipping young people with financial skills early, we lay the foundation for a generation less likely to fall into impulsive spending or dependency, creating a ripple effect that strengthens communities.

iv) Explore Insurance Options

Affordable products like health or funeral insurance can shield families from financial ruin. While often viewed as a luxury, insurance is a practical tool for protecting future savings.

Conclusion

Life is more than "YOLO." Enjoying today should not compromise tomorrow's security. The future will arrive whether we prepare for it or not, and the real risk lies in being unprepared when it does. Every Ugandan can mitigate this risk by taking small, deliberate steps today.

As the proverb says, "The best time to plant a tree was 20 years ago. The second-best time is now." ■

What phrase do you use to justify spending money without guilt?

OVER 1.5 MILLION WORKERS AT RISK OF LOSING THEIR NSSF SAVINGS

HARD WORK DESERVES A SECURE FUTURE.

Non-compliant employers should apply for Amnesty before *11th May 2026 to qualify for up to 100% penalty waiver.

Download the

Self Assessment Tool

from amnesty.nssfug.org or call 0800 286 773.

*After the deadline, full penalties and enforcement action under the law will apply. Act now to regularise your account.

NSSF a better life | 40 Years Making Lives Better

THE SILENT SUCCESSION

Israel Mubiru
Head of Risk & Compliance, AAR

Family-owned businesses are one of the pillars of East African economies such as Kenya, Uganda, and Tanzania. Yet many collapse after the founder's death due to poor or non-existent succession planning. According to an East African Business Survey 2023 by PwC, common challenges include disputes among heirs, operational paralysis, financial strain, and prolonged litigation.

The concept of "Silent Succession" offers a structured solution (quiet transition after death) by introducing senior and junior shareholding. This mechanism ensures smooth transition, preserves family harmony, and maintains business continuity. The structure relies on two main classes of shares:

Freezer (Senior) Shares – lock in the company's current value, guaranteeing founders a secure exit or retirement income.

Growth (Junior) Shares – allocated to heirs, entitling them to future business growth beyond the frozen value.

This approach aligns the founder and the heir's interests, reduces tax burdens, and minimizes conflict (HMRC, 2024).

Understanding Silent Succession

Silent succession is a low-profile succession strategy implemented during a founder's lifetime, avoiding the chaos that often follows death. It leverages differentiated shareholding to balance the financial security of founders with the growth incentives of heirs.

Senior (Freezer) Shares: Secure the founder's built-up equity and may include dividend or liquidation rights up to a set value.

Junior (Growth) Shares: Given to successors, often with nominal starting value, but tied to business expansion beyond the frozen equity.

Implementation typically involves amending company articles of association, creating the two share classes, and transferring junior shares to heirs. This gradual transfer keeps the process "silent," avoiding post-mortem disputes.

In jurisdictions such as Kenya, tax incentives such as business property relief have been proposed, mirroring the UK Business Property Relief model (HMRC, 2024).

Why It Matters: Preventing Litigation and Collapse

Without structured succession planning, founders' deaths often trigger disputes that destabilize businesses and economies. Senior/junior shareholding mitigates these risks by:

1. **Providing clarity –** freezing senior value prevents arguments over "fair" divisions.
2. **Aligning incentives –** heirs' wealth grows only if the business prospers.
3. **Preserving liquidity –** tax reliefs and phased transfers reduce forced asset sales.
4. **Reducing disputes –** proactive planning allows family dialogue before conflicts escalate.

According to the Family Business Institute (2023), only 30% of family businesses survive the second generation, and just 12% make it to the third, with succession failures being the main cause.

Real-Life Failures in East Africa due to inadequate planning:

- **Garuga Group (Uganda):** Following James Garuga Musinguzi's death in 2025, disputes erupted between heirs, threatening estate stability (Daily Monitor, 2025).
- **Tuskys Supermarket (Kenya):** Once a retail giant with 74 outlets and 6,000 staff, it collapsed in 2020 due to sibling rivalry and lack of succession planning after founder Joram Kamau's death (Business Daily Africa, 2020).
- **Njenga Karume Empire (Kenya):** The tycoon's estate fragmented after trustee mismanagement and litigation among heirs following his death in 2012 (Daily Nation, 2019).
- **Naivas Supermarket (Kenya):** Succession disputes among siblings and grandchildren escalated into costly litigation during a KSh 6 billion stake sale (Standard Media, 2024).
- **Nakumatt Holdings (Kenya):** Once East Africa's largest retailer, it collapsed in 2018 under KSh 38 billion debt, worsened by poor governance and family disputes (Business Daily Africa, 2018).

Successes with structured planning:

- **Bidco Oil (Kenya):** Smooth transition to second-generation leadership under Vimal Shah has driven revenues beyond $500 million (IFC, 2021).
- **Ramco Group (Kenya):** Still family-led with structured roles for heirs, maintaining turnover above $220 million (PwC, 2023).
- **METL Group (Tanzania):** Successfully transitioned to Mo Dewji, now leading a $1 billion conglomerate (Forbes, 2023).
- **Madhvani Group (Uganda):** Continues strong under structured succession planning led by Mayur Madhvani (IFC, 2021).

These contrasting cases show how structured transitions prevent collapse.

Comparing Traditional Methods

Silent succession via senior/junior shareholding offers advantages over other approaches:

- **Wills:** Often contested and slow due to probate (PwC, 2023).
- **Intestate succession:** Statutory division fragments businesses (Daily Nation, 2019).
- **Trusts:** Useful but prone to trustee disputes (Karume case).
- **Outright gifts:** Risky; heirs may sell or mismanage assets.
- **Buy-sell agreements:** Effective for partnerships but don't solve family disputes.

By contrast, silent succession ties heir wealth to growth, secures founders' retirement, and reduces litigation.

Conclusion

Silent succession provides East African family businesses with a powerful succession model. By combining clarity, fairness, and incentive alignment, it prevents litigation and collapse as seen in Tuskys, Nakumatt, and Karume's empire, while promoting continuity, as demonstrated by Bidco, Ramco, METL, and Madhvani.

In a region where family businesses contribute significantly to GDP and employment (IFC, 2021), adopting this model ensures sustainability, preserves legacies, and protects jobs for future generations. ■

BALANCING PROFITS WITH ESG REQUIREMENTS

Robert Masiga
Investment Risk Specialist, NSSF

In the contemporary financial arena, responsible investing, the integration of environmental, social, and governance (ESG) factors into investment decisions, has evolved from a peripheral consideration into a fundamental component of investment risk management. For professionals tasked with safeguarding assets, this approach is not merely about pursuing social good; it is a critical framework for identifying, quantifying, and mitigating material risks that threaten organizational long-term financial performance, sustainability and reputation.

This article examines the confluence of profit maximization on ESG requirements, explaining the growing need for responsible investing, implementation strategies, challenges and possible solutions.

The growing need for responsible investing

The momentum behind responsible investing is propelled by a growing body of evidence, according to UN Global compact, linking robust ESG practices to superior financial outcomes and operational resilience. Companies with strong governance and proactive environmental management practices are demonstrably better equipped to navigate regulatory shifts, operational disruptions, and potential reputational crises.

On the contrary, entities with weak corporate governance structures are more vulnerable to ESG challenges. The 2019 collapse of Vale S.A.'s Brumadinho dam in Brazil is a stark illustration. The disaster, a direct result of governance and oversight failures, resulted in catastrophic loss of life, environmental devastation, and a loss of over $19 billion in market capitalization for Vale within a month.

Another good example is the 2016 collapse of buildings in Nairobi's Huruma area, attributed to substandard construction materials and corrupt approval processes, which underscores the material financial and reputational risks of poor governance(G') that create negative

externalities. Investors with exposures in sectors that were affected, suffered significant losses.

Furthermore, a 2023 study by the Nairobi Securities Exchange (NSE) indicated growing investor appetite for sustainable products, especially by a younger and more digitally engaged demographic, that increasingly associates investment risk with corporate citizenship.

Risk Management Through an ESG Lens

Responsible investing empowers risk managers to address non-financial risks that pose profound financial consequences. These include:

Environmental Risks: Climate change presents a dual threat:

i. **Physical risks** e.g., prolonged drought, resulting in dwindling agricultural output in many parts of Africa. For example, the prolonged drought in Kenya, which severely impacted hydropower generation in 2020-2022, disrupted Kenya's agriculture sector, which contributes 20% to GDP and underpins many businesses in the country, especially agribusiness, leading to broader profitability pressures across the affected businesses, such as food processing, and related industries. This illustrates the direct material impact of environmental factors on portfolio performance.

ii. **Transition risks.** E.g., new carbon taxes or the sudden stranding of assets in the fossil fuel sector, as markets shift.

Social Risks: Labour unrest, community conflicts, and human rights abuses, etc., can devastate brand value and operational continuity. For example, M23 rebel capture of Walikale district in March 2025, forced mining suspension by Alphamin Resources, a Canadian Tin mining company in DRC. Due to security disruptions, workers were evacuated, and the community destabilized. Global media labelled Alphamin Resources as a "conflict mineral" supplier, considered to have exacerbated regional violence, damaging its reputation and prompting calls for audit of its supply chain, leading to a 15% share price drop and investor pullback.

Furthermore, according to Human Right Watch report of 2025, Jubilee Metals Group, a South African Lead/ Zinc mining company in Zambia, used child labor and caused toxic exposure at Kabwe site, with 95% of nearby children showing elevated lead levels.

As a result, the company has faced international outrage via Human Rights Watch reports, leading to delisting threats from sustainability indices and suffered reputational hits valued at $50M+ in lost partnerships, causing it to be branded as "legacy polluter" in global ESG rankings.

The aforementioned cases of social risks, highlight how social risks can translate into compliance violations, and impact international markets for companies and their investors.

Governance Risks: Weak board oversight, ethical lapses, such as lack of transparency and accountability, are potent precursors to financial scandals

and collapse. The historical downfall of Charterhouse Bank in Kenya in 2006, due to money laundering and tax evasion claims, remains a good case study in the East African region on how governance failures can lead to collapse of an institution, resulting in total loss for investors.

Integrating ESG analysis provides a forward-looking risk radar, enabling managers to mitigate exposure to volatilities and enhance portfolio durability.

Practical Strategies for responsible investing

To effectively embed responsible investing into risk frameworks, investors should consider:

1. ESG Integration

Systematically incorporate ESG factors into fundamental analysis and valuation models. For instance, during due diligence, a risk manager flags a company where the CEO also chairs the board (a lack of independent oversight). This governance weakness is factored into the valuation as a potential risk premium, prompting either a lower offer or a requirement for governance reforms before investment.

2. Active Engagement and Stewardship

These are operational pillars that transform ESG analysis from passive screening into proactive influence. They embed responsibility by turning investors from mere capital providers into agents of change within portfolio of companies. Shareholders should engage with investee companies, by making mandatory calls and site visits in high-risk areas and give timelines for resolution of identified issues, if no progress is made, decisions are made to vote against board chair or to divest during annual members' meeting.

3. Advanced Risk Assessment

Employ climate scenario analysis and risk mapping to stress-test portfolios against specific ESG risks, such as water scarcity or policy changes around single-use plastics, as is the case in countries like Tanzania and Rwanda.

4. Diligent Data Scrutiny

Leverage emerging frameworks and demand higher-quality disclosure to combat greenwashing. Regulatory bodies, such as the Capital Markets Authority of Kenya, are increasingly demanding for ESG disclosures, making robust data essential for accurate risk assessment.

5. Impact Investing

Allocate capital to investments designed to generate measurable, positive social or environmental impact alongside financial return. Affordable housing initiatives in Africa are taking shape through public-private partnerships, innovative financing, and a focus on sustainable building. Examples include the Housing Finance Bank (HFB) Zimba Challenge in Uganda, which promotes affordable home ownership through training and financial support, and the work of social enterprises like Smart Havens Africa, which builds climate-smart homes for low-income households, using sustainable materials and provides training to women. International organizations like the African Development Bank and UN-Habitat also support these efforts through funding, technical assistance, and housing policy development across the continent.

Despite the foregoing discussions, responsible investing faces a number of hurdles, including but not limited to:

1. Inconsistent Data

Inconsistent ESG data arises from varying reporting standards, methodologies across rating providers (e.g., MSCI, Sustainalytics), lack of mandatory auditing, and incomplete disclosures, making it difficult to compare companies or assess true sustainability performance.

Possible Solutions:

i) Adopt standardized frameworks and global convergence

Encourage widespread use of unified standards like the International Sustainability Standards Board (ISSB), Global Reporting Initiative (GRI), or Task Force on Climate-related Financial Disclosures (TCFD) to improve comparability and reliability.

ii) Leverage multiple data sources and aggregation tools

Investors can cross-reference ratings from various providers, use data aggregators, or employ AI-driven platforms for normalization and gap-filling.

iii) Enhance internal data management and verification

Asset managers should invest in robust ESG data systems, conduct independent audits, and prioritize primary company disclosures over third-party ratings.

iii) Push for regulatory mandates on disclosures

Support policies requiring assured, comparable ESG reporting (e.g., EU's Corporate Sustainability Reporting Directive) to reduce inconsistencies over time.

iv) Focus on material, industry-specific metrics

Tailor data collection to sector-relevant KPIs, reducing noise from irrelevant or inconsistent indicators.

2. Greenwashing

Greenwashing involves exaggerating or misrepresenting sustainability claims, eroding investor trust and leading to regulatory scrutiny, reputational damage, or financial penalties.

Possible Solutions:

i) Strengthen transparency and substantiation

Require detailed, verifiable evidence for ESG claims in marketing and disclosures, backed by third-party audits or certifications.

ii) Implement anti-greenwashing regulations

Enforce rules like the EU's Sustainable Finance Disclosure Regulation (SFDR), UK's Sustainability Disclosure Requirements (SDR), or U.S. Securities and Exchange Commission (SEC) guidelines, including fund labeling and minimum ESG investment thresholds, for instance, 80% alignment with named sustainability features.

iii) Conduct rigorous due diligence

Investors should scrutinize fund holdings, engage companies on ESG issues, and use tools like ESG controversies data to detect mismatches.

iv) Promote independent verification and ratings oversight

Regulate ESG rating providers for methodology transparency and regulate taxonomies (e.g., EU Taxonomy) to define "green" activities clearly.

v) Educate investors and set realistic expectations

Provide clear fund classifications (e.g., "impact" vs. "ESG integration") and disclose potential trade-offs to avoid misleading hype.

3. Regulatory Flux

Navigating emerging and evolving fragmented ESG regulations across different jurisdictions create compliance burdens, uncertainty, and cross-border challenges for global investors.

Possible Solutions:

i) Build flexible, forward-looking compliance systems

Establish dedicated ESG regulatory monitoring teams and use regtech/ AI tools for real-time tracking and automated reporting.

ii) Integrate ESG into governance and risk management

Embed regulatory preparedness into enterprise risk frameworks, including scenario planning for changes e.g., climate risk integration under Solvency.

iii) Advocate for harmonization

Participate in industry groups e.g., Principles of Responsible Investing (PRI), International Organization of Securities Commissions (IOSCO) to push for global alignment, such as International Sustainability Standards Board (ISSB) standards.

iv) Leverage technology for adaptability

Use scalable data platforms to handle multiple reporting templates and automate disclosures across jurisdictions.

4. Return Expectations

Balancing the often-long-term horizon of ESG benefits with short-term return pressures, remains a complex strategic challenge

Possible Solutions

i) Educate on long-term performance evidence

Research shows ESG-integrated portfolios often match or outperform traditional ones over time, with lower volatility (e.g., due to risk mitigation), especially globally.

ii) Focus on materiality and integration

Incorporate ESG as a risk/return factor rather than exclusionary screening - target companies where strong ESG drives profitability (e.g., better governance reduces scandals).

iii) Set blended objectives

Align client mandates with realistic goals for instance, risk-adjusted returns plus impact, using impact funds only where lower returns are accepted for measurable outcomes on ESG.

Conclusion

Responsible investing represents a paradigmatic shift in risk management. It is a disciplined approach that recognizes that long-term profitability is inextricably linked to sustainable and ethical business practices. For risk managers, the imperative is clear: integrating ESG factors is not a peripheral activity but a core strategic function, essential for protecting value, ensuring resilience, and capitalizing on the opportunities presented by the transition to a more sustainable global economy. ■

DERIVATIVES

THE MISSING KEY TO RESILIENCE IN EAST AFRICAN ECONOMIES

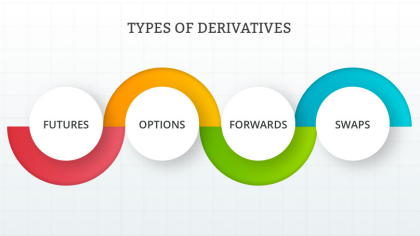
Michael Sendiwala
Senior Manager, Investment Risk, NSSF

Derivatives, the financial instruments whose value is derived from an underlying asset like a crop, a currency, or an interest rate, are often seen in developing economies as complex tools of advanced finance in more developed and sophisticated economies, and yet their fundamental role in managing risk is applicable even in emerging economies.

A derivative is essentially a contract between two or more parties, and its core element is its connection to another asset, known as the "underlying asset". The value of the derivative contract changes as the price of the underlying asset fluctuates in the market.

Derivatives are used for two primary purposes: One- to hedge against potential risks, two- to speculate on price movements. Businesses and individuals use derivatives to hedge against potential losses due to unfavorable price changes in an asset they intend to sell or buy in the future. For instance, grain farmers can use derivatives to hedge against expected fall in prices of the grain; an airline can use derivatives to hedge against rising fuel prices, etc.

The common types of derivatives include:



Futures: A contract to buy or sell an asset at a specific price on a future date on a regulated exchange.

Forwards: Similar to futures but are customizable and traded over the counter

Options: Gives the buyer the right, but not the obligation, to buy or sell an asset at a specific price by a certain date.

Swaps: Contracts that exchange one asset or cash flow for another, often used to manage interest rate or currency risk.

As stated above, derivatives are used for two purposes, risk management and speculation, however in this article, I focus on the derivatives' role in managing risks.

In East Africa, a region characterized by farming, rapid growth, and acute vulnerability to climate and global market shocks, derivatives can play a significant role in minimizing farmers' risks arising from price fluctuations, thus acting as a potential keystone for economic stability and sustainable development.

This article delves into the transformative risk management potential of derivatives for East Africa, exploring their practical use, diagnosing the significant challenges that hinder their adoption, and proposing actionable solutions grounded in both local context and international practice.

Why Derivatives Matter for East Africa

The volatility of global commodity prices, currency fluctuations, and climate variability, pose existential threats to East African businesses, farmers, and governments. Derivatives serve as a vital mechanism to transfer and mitigate these risks, offering a path to greater economic resilience.

Shielding Agricultural Economies: With a significant portion of GDP and employment linked to agriculture, price swings in commodities like coffee, tea, and maize directly impact national economic stability. Derivatives allow producers to lock in prices, ensuring predictable income and encouraging investment in productivity.

Catalyzing Capital Markets: The presence of derivatives makes the financial market more attractive to both foreign and domestic investors. A vibrant derivatives market signals maturity, deepens liquidity, and can lower the overall cost of capital for businesses.

Enabling Regional Trade Integration: As the East African Community (EAC) pushes for closer economic union, businesses engaged in cross-border trade face currency risk. Currency derivatives are essential for importers and exporters to hedge against adverse movements in exchange rates, facilitating smoother intra-regional commerce.

Promoting Financial Inclusion & Sustainability: By providing a mechanism for the smallest farmers and SMEs to manage risk, derivatives can be a powerful tool for financial inclusion. This aligns directly with the UN's Sustainable Development Goals (SDGs), protecting livelihoods and fostering climate adaptation.

Practical Use

The theoretical benefits of derivatives are made real through specific, actionable applications across East Africa's key sectors.

1. Agriculture: Securing the Harvest

Commodity Futures: A cooperative of Ugandan coffee farmers can sell futures contracts on a recognized stock exchange, locking in a price for their next harvest today. This protects them if global coffee prices plummet before delivery, as has happened historically.

International Parallel: In Brazil, large cooperatives like Minasul (located in Varginha, Minas Gerais), heavily use the Intercontinental Exchange (ICE) Futures U.S to hedge its exports, providing a model for price risk management.

Weather Derivatives: A Tanzanian maize farmers' association could purchase a derivative that pays out if rainfall in their region falls below a predetermined level. This payout acts as an insurance policy against drought, preventing crop failure from leading to financial ruin. One of the rainfall indexed insurance product is BIMA, which triggers low/excessive rainfall with automatic payouts for drought/ flood. The product covers maize and other crops during key growth stages like germination.

International Parallel: India, following catastrophic droughts, developed a successful rainfall index-based insurance scheme, demonstrating how financial instruments can be tailored to protect smallholders. Agriculture Insurance Company of India Limited is the leading provider of rainfall index-based insurance in India.

2. Foreign Exchange: Taming Currency Volatility

Currency Forwards: A Rwandan company importing pharmaceuticals priced in US dollars is required to pay $2million invoice in six months. To avoid the risk of the Rwandan franc (RWF) depreciating, it enters a forward contract with its bank to buy USD at a fixed RWF rate (RWF/USD=1,250) in six months, making its costs predictable.

Period	Scenario	Spot Rate in 6 Months (USD/RWF)	Cost without Hedge (RWF)	Action under Forward Contract	Importer's NET Effective Cost & Rate
6 Months Later	RWF DEPRECIATES	1,300	2,600,000,000	Buys USD at agreed 1,250 instead of market rate 1,300 Saving: 50 USD/RWF	RWF 2,500,000,000 Effective Rate: 1,250 USD/RWF **Saving: RWF100,000,000**
6 Months Later	RWF APPRECIATES	1,200	2,400,000,000	Must buy USD at agreed 1,250 instead of market rate 1,200 Opportunity Cost: -50 USD/RWF	RWF 2,500,000,000 Effective Rate: 1,250 USD/RWF **Opportunity Cost: RWF100,000,000**

Currency Options: A Ugandan horticulture exporter expecting to receive €1million in three months for its flower shipments, is worried about the euro weakening but also wants to benefit if it strengthens. By purchasing a put option on EUR/UGX, it pays a premium of UGX84million for the right to sell €1million at a guaranteed rate (EUR/UGX=4,200), capping its downside risk while retaining upside potential. This means that, if the UGX appreciated against the EUR by 200, the exporter will exercise the option to sell at the contract rate (4,200 instead of 4,000), thereby eliminating the loss. On the other hand, if the EUR appreciates against the UGX, the exporter will not exercise the option because the market rate is more favourable.

Period	Scenario	Spot Rate in 3 Months (EUR/UGX)	Revenue at Spot (UGX)	Option Decision & Cash Flows	Exporter's NET Effective Revenue & Rate
3 Months Later	**EUR WEAKENS**	**4,000**	**4,000,000,000**	**EXERCISE** the option. Sell EUR at **4,200** instead of **4,000**. Gain: +200 EUR/UGX	(4,000M from spot) + 200M gain - 84M premium = **4,116,000,000 UGX** Effective Rate: **4,116 EUR/UGX** **Gain: UGX116,000,000**
3 Months Later	**EUR STABLE**	**4,200**	**4,200,000,000**	Option is at-the-money. Let it expire or exercise for no gain.	4,200,000,000 - 84,000,000 = **4,116,000,000 UGX** Effective Rate: **4,116 EUR/UGX** **Opportunity Cost: = UGX84,000,000**
3 Months Later	**EUR STRENGTHENS**	**4,500**	**4,500,000,000**	**LET OPTION EXPIRE.** Sell EUR at the favorable spot rate of **4,500**.	4,500,000,000 - 84,000,000 = **4,416,000,000 UGX** Effective Rate: **4,416 EUR/UGX** **Gain: UGX416,000,000**

3. Energy & Infrastructure:

Commodity Swaps: A Kenyan fuel distributor is exposed to the volatile global price of crude oil. It can enter a swap agreement with a financial institution to pay a fixed price for oil (USD80 per barrel) over one year while receiving the floating market price. This swap effectively converts its variable costs into a known, stable expense.

Period	Scenario	Market Price (Floating)	Cost without Hedge	Cash Flows from Swap (per barrel)	Distributor's NET Effective Cost
Month 1	Prices are Stable	USD 80	USD 80	Pays USD 80 Fixed Receives USD 80 Floating Net Swap Flow: USD 0	(USD 80 from purchase) + (USD 0 from swap) = USD 80
Month 2	Prices RISE	USD 95	USD 95	Pays USD 80 Fixed Receives USD 95 Floating Net Swap Inflow: +USD 15	(USD 95 from purchase) - (USD 15 from swap) = USD 80
Month 3	Prices FALL	USD 65	USD 65	Pays USD 80 Fixed Receives USD 65 Floating Net Swap Outflow: -USD 15	(USD 65 from purchase) + (USD 15 from swap) = USD 80

Interest Rate Swaps: A Ugandan developer building a major NSSF project secures a large loan with a variable interest rate, exposing it to rising rates. Through an interest rate swap, it can agree to pay a fixed rate (10%) to a counterparty in exchange for receiving a floating rate (3 months Treasury bill rate), thus hedging against rising interest costs and ensuring project viability.

Period	Scenario	3-Month Treasury Bill rate (TB)	Loan Interest Rate (TB rate + 3%)	Cash Flows from Swap	Developer's NET Effective Rate
Year 1	Rates are Stable	10.00%	13.00%	Pays 10.0% Fixed Receives 10.0% TB Net Swap Flow: UGX 0	(13.0% from loan) + (0% from swap) = **13.0%**
Year 2	Rates RISE	12.00%	15.00%	Pays 10.0% Fixed Receives 12.0% TB Swap Inflow: +2.0%	(15.0% from loan) - (2.0% from swap) = **13.0%**
Year 3	**Rates FALL**	8.00%	11.00%	Pays 10.0% Fixed Receives 8.0% TB Net Swap Outflow: -2.0%	(11.0% from loan) + (2.0% from swap) = **13.0%**

Challenges: The Steep Hurdles to Adoption

The potential of derivatives is immense, but the path to a functional market is fraught with obstacles which include;

a. **Regulatory and Legal Immaturity:** The framework for enforcing complex derivative contracts is underdeveloped. The legal enforceability of close-out netting (a key process in managing the risk of default) is uncertain in countries like Uganda and Tanzania, creating high legal risk for participants.

b. **Profound Financial Literacy Gap:** In developing markets such as the Ugandan market, there is generally complete lack of knowledge of what the derivatives are and how they can be used for risk hedging/ mitigation or speculation.

c. **Underdeveloped Financial Infrastructure:** East African exchanges (e.g., Nairobi Securities Exchange's derivatives segment) are emerging but suffer from low liquidity, making it expensive to enter and exit positions. The lack of a robust central counterparty clearing house for over the counter (OTC) trades, exacerbates counterparty credit risk.

d. **Systemic and Operational Risks:** In markets with weak oversight, the misuse of leveraged derivatives could amplify risks rather than mitigate them. Furthermore, the high cost and complexity of these products often exclude the very smallholders and SMEs who need them most.

Possible solutions

Overcoming these challenges requires a concerted, multi-stakeholder approach, and below are some of the solutions.

a. **Build Robust Regulatory Frameworks:** The EAC member states need to harmonize derivatives regulations and explicitly affirm the legal enforceability of netting agreements. Adopting standards from the International Swaps and Derivatives Association (ISDA) would provide immediate credibility and attract international players.

b. **Prioritize Financial Education:** Banks, exchanges, professional bodies and governments need to take deliberate steps to create targeted (Co- operatives and SME) awareness of the derivatives. Mobile-based learning platforms and training through saving groups and other cooperatives can demystify derivatives for end-users, reframing them as insurance, not speculation.

c. **Invest in Core Infrastructure:** The establishment of a regional central counterparty clearing house is non-negotiable for mitigating counterparty risk and building trust. Furthermore, investing in technology for exchanges can enhance transparency, reduce costs, and improve liquidity.

d. **Promote Product Innovation and Accessibility:** Financial institutions should be encouraged to develop "micro-derivatives" or bundled products with lower entry barriers. Public-private partnerships could initially subsidize transaction costs for farmers to kick-start adoption, similar to agricultural subsidy programs.

> **International Parallel: The success of Mexico's Cadenas Productivas program, which taught farmers to use futures contracts with government support, offers a valuable case study in building a hedging culture from the ground up.**

Conclusion

Derivatives represent a profound opportunity for East Africa to rewrite its economic narrative, from one of vulnerability to global forces to one of managed risk and confident growth. The journey from an embryonic to a mature derivatives market is complex, requiring unwavering commitment to regulatory reform, financial education, and infrastructure investment. By learning from global successes and failures and tailoring solutions to local realities, East Africa can harness these powerful financial instruments to protect its farmers and empower its businesses. ■

EMERGING RISKS IN THE FINANCIAL INDUSTRY IN UGANDA

IMPLICATIONS FOR BANKS

Ronald Kayizzi
Head of Risk, Bank of Africa

The financial sector in Uganda has seen a marked evolution over recent years, driven by digital innovations, regulatory reform, expanded financial inclusion, and global inflows. The environment offers abundant opportunities but it also heralds a new frontier of emerging risks. For financial institutions entrusted with safeguarding customers' deposits and at the same time having a duty to create value for shareholders, through lending customers' deposits, they find themselves on a tight balance. They should, therefore, proactively seek to understand the nature and severity of the various risks, and take appropriate measures to address them in a timely manner.

Below are six key risk categories that warrant attention, along with illustrative data, in the Ugandan context.

1. Technology & Cyber Risks

As digitization accelerates, financial institutions are exposed to novel threats. Uganda's experience highlights both opportunities and perils.

A policy brief from Gateway Research Centre titled - "The Quest for Cyber Security to Combat Threats to Digital Finance in Uganda" (May 2023), highlights how banks, remittance platforms, and telecom companies in Uganda are key targets for cybercriminals (hackers, phishers, fraudsters).

Technology adoption in Uganda has grown rapidly, driven by expanding internet access, mobile money, e-government services, and a young, digitally active population. However, this growth has come with rising cyber threats, including mobile money fraud, phishing attacks, SIM-swap scams, ransomware incidents, and data breaches, targeting both individuals and institutions, in addition to new AI related fraud. As more services move online, gaps in digital literacy, weak cybersecurity practices, and limited enforcement capacity make users more vulnerable.

Strengthening cybersecurity awareness, enforcing data-protection standards, and investing in secure digital infrastructure, are essential for protecting Uganda's digital ecosystem.

PwC Uganda notes that BoU's new ICT/ Cyber Risk Management Guidelines (requirements effective December 2024) mandate financial institutions to put in place robust governance, cyber testing, and technology risk management practices. Addressing AI fraud requires continuous updates to regulatory frameworks, enhanced detection mechanisms, and increased public awareness. Raising awareness about the risks associated with it is crucial.

SIM swap fraud is being used to not only steal credentials and capture one-time passwords (OTPs) sent via an SMS, but also to cause financial damage to victims by resetting the accounts and allowing fraudsters to access currency accounts not only in banks, but also in Fintechs.

Implications for banks:

- As banks invest and work through digital channels (whether internet banking, mobile wallets, card services, or data analytics), the cyber risk landscape needs special attention.

- Data breaches, authentication failures, and fintech vendor vulnerabilities, can lead to reputational damage, regulatory cost and loss of customer trust - all of which undermine long term sustainability.

- Integrating strong IT governance, vendor oversight, scenario stress testing of cyber events, and continuous training, are critical in mitigating this risk.

- As fintech and digital credit proliferate, banks must assess their exposure to protect customers against this risk and possible systemic fallout.

2. Climate change risks

While often considered non traditional, climate risk is increasingly becoming a financial risk - especially in an economy like Uganda. The Country Climate and Development Report (CCDR) by the World Bank shows that without strong action, climate change could cut Uganda's economic growth by up to 3.1 % by 2050, push more than 613,000 people into poverty, and create 12 million internal migrants. Climate and environmental risks directly impact financial institutions at micro and macro (systemic) perspectives.

Climate change can impair borrowers' ability to repay loans, leading to defaults and higher non-performing loans (NPLs). Physical risks like floods, droughts, and storms destroy assets that serve as collateral or income sources.

For example, a commercial bank faces a high risk of default if it finances farmers or agro - processors in Eastern Uganda, and the region experiences droughts or heavy rains that reduce yields.

Another example is the recent (November 2025) incident in downtown Kampala, where traders lost merchandise worth hundreds of millions of shillings due to a heavy downpour that caused severe flooding that wrecked their shops. If the affected traders had loans, their ability to repay the loans would be compromised, since their source of income was destroyed. The FDIC (Agricultural lending, insurance, and implications of climate change, CFP/ working paper, 2024), shows that climate impacts (droughts and floods) increase agricultural loan delinquency and may push lenders to restructure production loans into longer-term debt.

Transition risks (policy or market shifts due to the move toward low-carbon economies) can make some business models obsolete or less profitable. For example, a bank financing fuel distributors, diesel-powered manufacturing, or non-renewable energy investments, might see higher credit risk as Uganda scales up solar and hydro projects, or if future carbon pricing raises costs. Climate risk

> **Without strong action, climate change could cut Uganda's economic growth by up to 3.1 % by 2050, push more than 613,000 people into poverty, and create 12 million internal migrants.**

results in higher provisioning for loan losses, leading to reduced profitability. The regulator of the financial sector in Uganda is developing climate risk guidelines and climate stress testing tools to help supervised financial institutions identify and mitigate these risks.

Agriculture accounts for more than 70 % of livelihoods in Uganda. Floods, droughts and other weather disruptions are now being treated as credit/loan recovery risks by banks. For example, a "climate smart" shift in credit assessment is underway: banks now consider that "a farmer who can't predict rainfall patterns is a higher risk borrower".

Implications for banks:

- As banks lend to businesses which invest in agriculture, infrastructure, real estate or natural resource linked assets, physical climate risk (floods, droughts, heat stress) and transition risk (regulation, pricing of carbon, ESG demands), they must factor in ESG risks in their credit risk assessment and portfolio valuation.
- Scenario analysis and stress testing for climate driven shocks (e.g., crop failure, property damage, stranded assets) should be incorporated.
- Wider disclosure and integration of ESG metrics will enhance transparency to members and stakeholders, aligning with global best practice.

3. Regulatory & Compliance Risks

Financial institutions operate in a dynamic regulatory environment. For Uganda, as the sector matures, regulatory complexity is increasing. The pace of regulatory change has accelerated - both locally and globally, creating pressure on financial institutions to continuously adapt new policies, systems, and reporting frameworks. Basel III/IV Liquidity & Capital Requirements have dictated the implementation challenges in maintaining Liquidity coverage ratio (LCR) and the Net Stable Funding ratio (NSFR), especially in smaller banks with limited high-quality liquid assets.

IFRS 9 (Credit Loss Provisioning) has caused a complexity in modeling Expected Credit Losses (ECL) and integrating forward-looking data. Anti-Money Laundering & Countering the Financing of Terrorism (AML/CFT) has increased scrutiny from global bodies like the Financial Action Task Force (FATF), and local and regional regulators.

In Uganda, the Financial Intelligence Authority (FIA) has intensified compliance audits, and penalties for non-compliance have risen sharply. Political and governance risk also translate into regulatory risk.

Implications for banks:

- Financial institutions must maintain robust regulatory risk monitoring - covering AML/CFT, fintech oversight, ESG disclosure, and evolving central bank supervision.
- Non compliance (for example, inadequate data protection, disclosure lapses, poor governance) carries fines, reputational damage and possibly curtails investment avenues.
- Regular horizon scanning, scenario modelling for regulatory shocks, and ensuring internal capacity for compliance are imperative.

4. Macroeconomic & Market Risks

The macro environment remains a foundational risk driver and Uganda is not immune to external shocks. Although Uganda's financial sector remains resilient (customer deposits hit UGX 38 trillion; liquidity buffers remain healthy), risks remain from currency depreciation, inflation and global financial conditions(The Cooperator News). Market risks include asset price volatility, bond yield shocks, commodity price swings, etc.

Implications for banks:

- Inflows from depositors and investment returns from fixed income securities can be significantly affected by macro shifts (inflation eating real value, currency depreciation reducing foreign asset value, interest rate affecting bond portfolios).
- Large investment portfolios become increasingly difficult to liquidate in stressed markets, creating a liquidity risk.
- Diversification, scenario stress testing (including high inflation, currency depreciation, rate shocks) and a liquidity buffer strategy become crucial.

5. Operational, Human Capital & Outsourcing Risks

Even with strong strategy and markets, internal weaknesses pose risk. A core challenge in Uganda's evolving financial ecosystem is capacity. As products grow in complexity (fintech, ESG, digital lending), the shortage of skilled personnel increases risk. Operational risk manifests through weak processes, manual legacy systems, inadequate controls, and fraud vulnerability - especially given the digital shift. For example: The Banking Stability Review report shows that while payments grow rapidly, agent banking growth of 48.7% is accompanied by a drop in active agents, signaling possible governance or incentive issues.

As financial institutions increasingly rely on third-party vendors to deliver critical services - from cloud hosting and payments processing to cybersecurity and customer support - outsourcing risk has become a central concern for regulators and risk managers. Outsourcing can improve efficiency and reduce costs, but it also creates new vulnerabilities that can threaten operational resilience, data integrity, and compliance.

Third-party vendors and mobile infrastructure are critical risk points for banks, offering digital payments/ mobile wallets. Vendor/third party risk, agent banking risk, mobile money channel risk; are all types of cyber exposures, resulting from outsourcing.

There are external service providers who connect to banks' systems or process information on the banks' behalf - for example:

- Core banking vendors, cloud service providers, FinTech partners, or mobile aggregators like Pegasus or Yo! Uganda. Vendors might not maintain the same cybersecurity standards as the banks, exposing the banks to cyber-attacks via counterparties' systems.
- Sensitive bank customer data stored on third-party servers could be stolen in case a vendor is compromised.
- Supply-chain attacks, where hackers insert malicious code or updates into legitimate software provided to the bank (for example SolarWinds-type attacks)
- Agents' POS terminals or smartphones can be infected with malware that captures credentials or transaction data. Weak authentication where agents often use shared logins or unsecure Wi-Fi connections, which can be intercepted.
- Fake agents/identity theft where fraudsters clone agent IDs or intercept communication between agent devices and the bank (man-in the-middle).

A growing share of core financial infrastructure is handled by a small number of dominant service providers, particularly in cloud computing, and system integration. This creates systemic concentration risk: a single provider failure, cyber incident, or prolonged outage can simultaneously impact large parts of the financial sector.

Many banks outsource various services to external providers, but it is important to note that outsourcing transfers responsibility for the outsourced functions but not accountability. Institutions may lose visibility into the service provider's processes, controls, staffing, or security posture. Poor oversight increases the chance that errors, service degradation, or control failures go unnoticed until they cause significant harm to the banks.

Vendor disruptions (financial distress, operational outages, staffing shortages, mergers, or strategic shifts) can impair a bank's ability to serve customers. Robust business continuity and disaster recovery arrangements across the vendor ecosystem are crucial.

Moving away from an incumbent provider - especially cloud or core system providers, can be costly, complex, or operationally disruptive. This lock-in effect increases long-term dependency and reduces bargaining power, while making exit strategies difficult to implement.

Implications for banks:

- As the banks do their business of financial mediation, ensuring due diligence, strong operational controls, vendor oversight and human capital investment is non negotiable.
- Succession planning, continuous training (especially on emerging domains like ESG and digital investing), and embedding robust internal control frameworks will reduce risk of loss, error or reputational damage.
- Monitoring third party risk (service providers, fintech vendors, asset managers) with the same rigour as internal operations is vital.

6. Behavioural & Social Risks

Emerging risks are not just about markets and processes - they are also about people and society.

As digital inclusion deepens in Uganda, consumer expectations rise. All bank stakeholders (customers, employees, shareholders, the regulator) and society at large expect transparency, responsiveness and value for money from banks and financial institutions. If these expectations are unmet, reputational risk grows. Digital lending risks (over indebtedness, predatory practices) may have knock on effects on the financial institution's health. Social media and public sentiment can escalate minor issues into major reputational crises.

Implications for banks:

- The banks and other financial institutions must maintain active stakeholder engagement through proper communication.
- Ethical investments, inclusive behaviour, transparent structures and responsiveness to customers' concerns strengthen resilience.
- Customer behaviour analytics, feedback loops, and proactive reputation management frameworks help mitigate social risk.

Conclusion

Emerging risks in Uganda's financial sector are not distant theoretical concepts; they are active, evolving and real. For institutions like banks, which have both a fiduciary mandate and a social purpose, building a forward looking risk management framework is an imperative. Such a framework must integrate governance structures that reflect a paradigm shift, that is forward-looking, and a culture of resilience and adaptation. ■

CYBERSECURITY AWARENESS BEYOND THE OFFICE

Pauline Kire
Cybersecurity Engineer, Stanbic Bank Uganda &
Founder of TheCyberMamushka

One Digital World

We live in a time when our personal and professional lives are more connected than ever before. The smartphone you use to approve a business transaction in the morning might be the same one your child borrows to watch cartoons in the evening. A click on a suspicious link in your personal email could open the door to risks that affect not only you, but also your workplace.

Cybersecurity is no longer confined to the IT department or the server room. It touches everyday aspect of our lives; from how we protect our children on social media, how employees handle sensitive company data, and how communities safeguard themselves against digital scams.

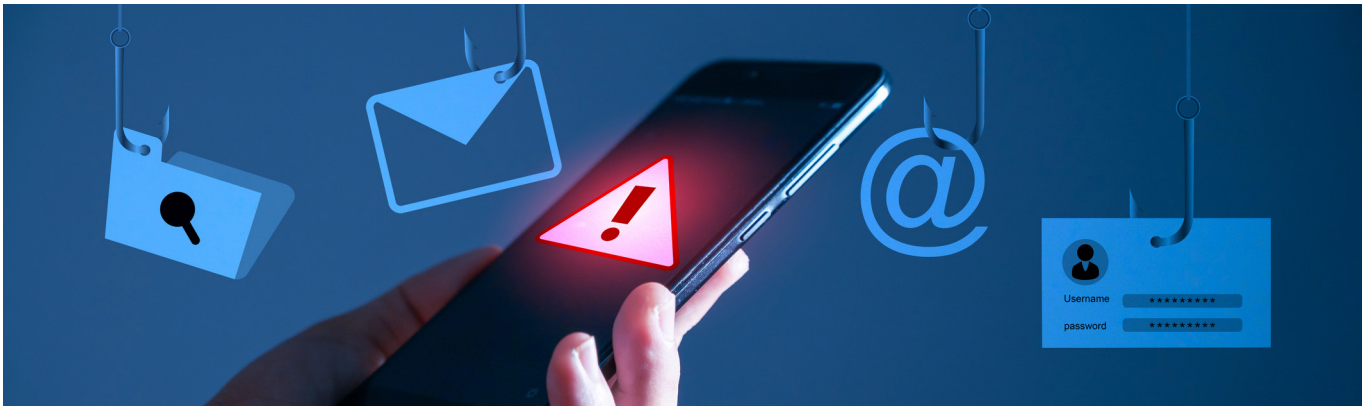
This article explores why cybersecurity awareness is critical in both the corporate space, the family and community spaces. By understanding the overlap, we can see that building a culture of security isn't just about compliance or technology; it's about protecting people, organizations, and society. Firstly, let us look at;

i) Cybersecurity in the corporate space

In organizations today, cybersecurity is not just about IT teams running scans or installing firewalls; it's about every employee recognizing their role as a digital gatekeeper. With the rise of phishing, ransomware, and insider threats, a single click on a malicious link can compromise sensitive customer data, interrupt operations, or even damage the company's reputation.

That's why leading organizations are shifting their focus from one-time training sessions to building a culture of security awareness. This means:

- **Phishing Simulations & Continuous Training:** Employees need more than an annual workshop. Regular, scenario-based simulations help staff practice spotting suspicious emails, links, and attachments.
- **Leadership Buy-in:** When executives champion cybersecurity, employees take it seriously. Leaders who model good security habits like using MFA or reporting phishing, set the tone for the entire organization.
- **Role-Based Awareness:** Not everyone faces the same risks. A finance officer might be targeted with invoice fraud, while developers



need to focus on secure coding and access controls. Tailored awareness ensures that training feels relevant and practical.

- **Third-Party Vigilance:** Modern businesses rely on third-parties for provision of various services, such as internet connectivity, consultancy, insurance, etc. If one of these partners' systems is compromised, your organization could be at risk. Embedding cybersecurity checks in procurement and vendor management is now a must.

Corporate cybersecurity awareness is ultimately about empowering people with knowledge. Technology may detect and block threats, but the human layer remains the most critical and often the most targeted. When employees understand the "why" behind security measures, they're more likely to practice them consistently, both in the office and beyond.

ii) Cybersecurity in the Family & Community Space

When the word "cybersecurity" is mentioned, many people imagine big companies, servers, and hackers in hoodies. But the truth is, digital threats live with us every day in our homes, schools, markets, and shopping malls.

Think about a typical day in Kampala or any Ugandan town. You stop by Nakasero market and pay a vendor using mobile money. At Owino, someone offers you a "cheap deal" on a phone, asking for a deposit via a mobile wallet. Or at a local garage, a mechanic borrows your phone to check a spare part online. These might seem like normal community interactions but they're also moments where cyber risks can sneak in.

Here's what community-level cybersecurity awareness looks like:

- **At the market:** Be cautious of mobile money fraudsters who might ask you to reverse transactions or give out your PIN. Always confirm the recipient's name before sending money.
- **At the mall:** Free public Wi-Fi is tempting, but it's not always safe. Avoid logging into your bank app or email over open networks without a VPN.
- **At the garage or shop:** Think twice before handing over your unlocked phone to someone "just to check" something, it only takes seconds to install a malicious app.
- **At home with family:** Children and teens are online more than ever. Teaching them not to share passwords, personal photos, or school details with strangers is just as important as reminding them to look both ways before crossing the road.

In the same way companies build a security culture to protect their data and systems, families and communities need everyday cyber hygiene. It doesn't require advanced tools, sometimes it's as simple as double-checking a message before sending money, keeping software updated, or having honest conversations about online risks at home and in our local circles.

By normalizing these practices, we create a ripple effect. The habits we develop at home influence how we behave at work, and vice versa. Safe families mean safer communities, and safer communities mean safer workplaces.

Bridging the Two Worlds

Cybersecurity awareness is often treated as if it belongs in two separate silos, the corporate environment and the personal/community space. In reality, these worlds are tightly interconnected, especially in a country like Uganda, where mobile money, smartphones, and digital services are part of both work and everyday life.

> **When executives champion cybersecurity, employees take it seriously.**

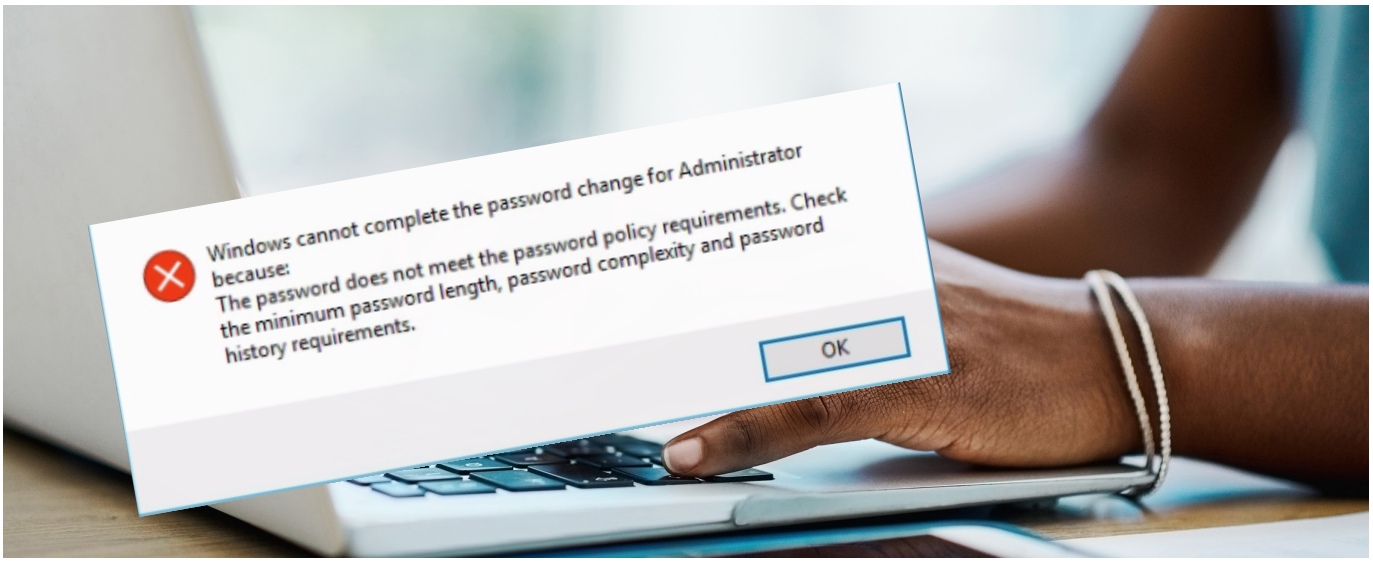
When an employee learns to recognize a phishing email through a corporate training program, that same skill helps them avoid falling victim to mobile money scams in local markets or shopping malls. Similarly, when families practice safe digital habits, teaching children not to share passwords, being cautious with unsolicited WhatsApp links, or using secure payment methods at local shops and garages, these behaviors follow individuals into the workplace, reducing the risk of corporate compromise.

This cross-over matters because threat actors don't see boundaries. A compromised personal account can be the entry point into a company's systems. Similarly, a careless action at work can have ripple effects at home, such as leaked personal information or fraud attempts targeting family members.

By embracing cybersecurity awareness as a shared responsibility across offices, homes, and communities, we move from isolated pockets of defense to a united front. Just as communities in Kampala, Entebbe, or Gulu look out for each other in physical spaces, we need the same vigilance in the digital spaces we all depend on.

Practical Steps to Address the Challenge

Awareness is most powerful when it translates into daily practice. Whether you are managing sensitive customer data in a bank or helping a child set up their first smartphone, the principles are the same: be alert, be proactive, and protect what matters.



Here are some practical steps that cut across both corporate and community life.

1. **Use Strong & Unique Passwords**

- **Corporate:** Encourage staff to avoid password reuse across business applications and personal accounts.
- **Family/Community:** Parents can model this by using password managers for their personal banking apps, e-commerce accounts, or social media logins. A compromised Facebook account at home could be used to launch scams that also target colleagues at work.

2. **Enable Multifactor Authentication (MFA)**

- **Corporate:** Enforce MFA for remote access, email, and privileged accounts to reduce the risk of breaches.
- **Family/Community:** Encourage everyone, even your teenager with a TikTok account to turn on MFA. In Uganda, where SIM-swap fraud is rising, using app-based authenticators instead of SMS adds extra safety.

3. **Be Scam-Smart**

- **Corporate:** Train employees to recognize phishing attempts, fake invoices, and suspicious links.
- **Community:** In our local markets, be wary of anyone asking you to "reverse" a mobile money transaction or send money to claim a prize. The same caution we practice at work applies at the Owino market, in the taxi park, or when paying for a boda ride through mobile money.

4. **Update & Patch Regularly**

- **Corporate:** IT teams should roll out updates to servers, applications, and endpoints to close vulnerabilities.
- **Family/Community:** Keeping your smartphone updated, even if data is expensive, helps block malware that criminals use to steal contacts, photos, or financial details.

5. **Promote a Culture of Speaking Up**

- **Corporate:** Employees should feel safe to report suspicious activity without fear of blame.
- **Community:** If someone in your neighbourhood or church group receives a scam message, sharing that knowledge could protect others from the same trap.

When organizations, families, and communities practice the same habits, the barriers against cybercriminals multiply. The safer we are at home, the safer we are at work and vice versa.

So, what is the way forward?

Cybersecurity awareness is not a one-time campaign; it's a continuous journey that requires everyone's involvement. The threats we face as employees, parents, business owners, and community members, are interconnected, which means our defenses must also be interconnected.

Here's how we can take the next step, wherever we are:

- For Organizations: Move beyond check-the-box compliance. Invest in regular, engaging awareness programs, empower employees to report incidents without fear, and extend cybersecurity resources to staff families. A workforce that feels supported at home will be more resilient in the office.
- For Families: Make digital safety a part of daily life, just like locking the front door. Talk to your children about safe online behaviour, help relatives recognize scams, and encourage everyone to use strong passwords and multifactor authentication.
- For Communities: From local markets to churches and schools, we can share knowledge with neighbors and friends. A quick conversation about fake SMS messages or mobile money scams could save someone from losing their savings.

Conclusion

Cybersecurity awareness is no longer optional or confined to the workplace. In a digitally connected society, personal habits, family practices, and organizational controls are inseparable. By embedding cyber-safe behaviors into our daily routines, from local markets to corporate offices, we build resilience not just for ourselves, but for the wider digital ecosystem we all depend on. ■

Access NSSF services in your neighbourhood.

With **over 20,000** Quickteller agents across Uganda, now you can:

- Register for Smartlife Flexi
- Make NSSF payments
- Make contributions to Smartlife Flexi

For more information call **0800 286 773** toll-free or visit **www.nssfug.org/nssftulikukyaalo**

Powered by Quickteller

NSSF a better life

40 Years Making Lives Better

PUZZLE ISSUE NO.10

1	2	3	4		5	6	7	8
9				■	10			
11				12			■	
13		■	14				15	
16		17		■	18			■
■	19			■	20			21
22	■		■	23		■	■	
24			25		■	■	26	
	■	27			28	29		
30			■	31				■

DOWN

1. Capital raised by a company through the issue of shares,5
2. Combined to form a single entity,6.
3. Wing in Latin,3
4. Profit or loss on an investment,6
5. Of considerable or relatively great size, extent, or capacity,7
6. A global network for academics, researchers, and professionals focused on purchasing and supply chain management, abbr.6
7. Chemical symbol for iron, 2
8. A way out of a building,4
12. Used to link alternatives, 2
15. Acts as the price to buy or sell units in open-ended funds, abbr. 3
17. Hollow containers used to give shape to molten or hot liquid material when it cools and hardens,6.
21. Slave or servant in Hebrew, 4
22. A device or enclosure designed to catch and retain animals, typically by allowing entry but not exit or by catching hold of a part of the body,4
23. Space that can be occupied,4
25. The practice of managing and disseminating information to the public, abbr. 2
26. A new or revived form of,3
28. In finance, a key stock valuation metric showing how much investors pay for $1 of a company's earnings, abbr. 2
29. In finance, a professional who handles investment portfolios for clients, making decisions on asset allocation, buying/selling, and risk management to meet financial goals, abbr. 2

ACROSS

1. NSSF's voluntary, goal-based savings plan,9
9. Relates to or at a distance,4
10. A climax, 4
11. Public speakers, 7
13. Digital visuals, abr.2
14. Requiring immediate action or attention,6
16. In medical, refers to surgery to repair the knee's tendons, often improving, function, (Knee Extensor Mechanism Reconstruction),4
18. A government body that regulates electricity in Uganda, abbr.3
19. University senior male teacher, 3
20. Set aside a portion of income not used for current spending,4
23. Refers to immediate processing, abbr. 2
24. Roman Law of Property and Obligations, abbr.5
26. Chemical symbol of Neon, 2
27. Made low or lower than usual,7
30. Refers to a place and system where retail transactions happen, abbr.3
31. A written message within an organization,4

SOLUTION TO ISSUE NO. 9

A	P	P	E	T	I	T	E	■	S
C	E	L	L	■	F	R	A	M	E
T	R	A	N	S	F	E	R	S	■
I	C	I	■	C	Y	A	N	■	A
V	■	N	T	H	■	D	E	A	L
E	■	S	O	O	T	■	D	V	L
■	L	■	R	O	A	D	■	A	E
P	A	I	■	L	R	■	R	I	G
A	T	L	A	S	■	P	O	L	E
T	E	L	L	■	B	L	I	S	S

THE CYBER Mamushka

CYBER SAFETY BEGINS AT HOME—

AND YES... EVEN ON YOUR PHONE RIGHT NOW.

Simple, practical ways to protect what matters most—
your family, your money, and your peace of mind.

"Most cyber incidents don't start with hackers—they start with **people.**"

How We Help You Stay Safe Online

- **Cyber Safety Awareness That Actually Makes Sense**
  No jargon. Just real-life habits you can use every day.
- **Interactive Learning (Courses, Quizzes & Tools)**
  Learn, test yourself, and build confidence online.
- **CyberSafe or CyberSorry Card Game**
  Because learning cyber safety shouldn't be boring 😉
- **Checklists, Guides & Digital Tools**
  Quick wins you can apply immediately
- **Incident Response Support**
  When something goes wrong, you don't have to figure it out alone

---

Explore tools, guides & resources
to help you stay safe:

www.thecybermamushka.com

paulinekire@thecybermamushka.com

0701550243

Mutungo Hill View Drive, Butabika

14th Floor, Workers House,
Plot 1, Pilkington Road,
P.O.Box 7140 Kampala, Uganda.

Tel: **0313 331755**
Toll-Free: **0800 286 773**
WhatsApp: **0784 259 713**
Email: **customerservice@nssfug.org**

www.nssfug.org