

The RiskEcho

ISSUE 8 - FEBRUARY 2024

Intriguing Insights





RISK



Disclaimer:

The National Social Security Fund (NSSF) does not take responsibility for the accuracy and authenticity of the articles written by the various parties in The Risk Echo magazine, and the publication of an advert in the magazine, except NSSF adverts, does not mean an endorsement of a product or service by the NSSF.



FOREWORD

At the Fund, we welcome 2024 with a lot of optimism and great relief, having gone through the most challenging time since the new dawn at the Fund in 2010, that saw the coming of new management that has transformed the Fund from an asset base of UGX1.7 trillion in 2010, to UGX 18.56 trillion by 2023.

The crisis that engulfed the Fund for nearly five months, from January 24, 2023, to June 30, 2023, when the IGG released its investigation report, was triggered by a Parliamentary probe that commenced on January 24, 2023 into the allegations of corruption and mismanagement at the Fund. In a public inquiry, telecast by all the media in the country, Parliament interrogated nearly all who matter in the Fund, including but not limited to the Board members, Managing Director, Deputy Managing Director, Heads of departments, senior managers, and other staff. The Fund's operations were greatly affected, staff morale was at its lowest and the Fund's positive media tonality dipped to as low as 21% from 97% in the previous quarter.

Although Parliament found most of the allegations as false, they raised various other issues, and directed the IGG to carry out deeper investigations. Fortunately, the IGG did not find evidence on nearly all the issues Parliament had raised, although the

IGG made some recommendations for process improvements.

Following the issuance of the IGG report on June 30, 2023, which by and large, exonerated management of the Fund of wrongdoing, the Fund's positive media tonality shot up to 80%.

In addition, other entities such as the Office of the Auditor General and the URBRA, etc., conducted parallel investigations into similar allegations. Such was 2023 for the Fund!

Despite that crisis and the challenging market conditions, exacerbated by the effects of the Covid-19 and the ongoing war between Russia and Ukraine, that affected global supply chains, leading to runaway inflation around the globe, the Fund performed very well. This is attributed to a robust risk management culture in the Fund. Assets under management grew to UGX18.56 trillion (2022/23) from UGX17.26 trillion (2021/22), and cost of administration reduced by 0.15%, from 1.18% (2021/22) to 1.03% (2022/23), among others. But most importantly, the Fund was able to declare a 10%-interest rate for its members, which reflected an increase of 0.35%, compared to the previous year.

The year 2024 brings us closer to the end of our 10-year strategic journey, in which we set ourselves to grow the

asset base to UGX20 trillion, reduce turnaround time (TAT) on processing benefits to 1 day, increase customer and staff satisfaction to 95%, by 2025. As we closed 2023, the Fund's asset base stood at UGX19.55 trillion, customer and staff satisfaction scores were 88% and 86%, respectively, and TAT averaged at 11.1 days.

As 2025 approaches, our attention is now on the next journey, which is 2025 to 2035, for which we have set ourselves an ambitious target of 50:50: 95; that is, increase asset base to UGX50 trillion, increase social security coverage to 50% of labour forces and increase stakeholder satisfaction to 95%.

This is an ambitious target indeed, because in the current strategic journey we planned to grow the assets by an average of UGX1.44 trillion per year, from UGX5.6 trillion 2015 to UGX20 trillion by 2025. In 2025 to 2035, we expect to grow the assets by UGX3 trillion annually!

Finally, I wish you a happy and prosperous new year, 2024, and I encourage you to save for a better life.

Edward Senyonjo
Chief Risk Officer - NSSF

S T R E N G T H E N I N G C O N

Pg 01

Q&A WITH MILTON STEVEN OWOR

The Chief People & Culture Officer - NSSF

Pg 08

2023: A YEAR IN REVIEW

Pg 13

**CYBER EXTORTION
NAVIGATING A RISING
THREAT LANDSCAPE**

Pg 15

**SHAPING YOUR
FINANCIAL FUTURE
THE ART OF STRATEGIC
ASSET ALLOCATION**

Pg 17

**HOW TO REINFORCE
ANTI-MONEY LAUNDERING
COMPLIANCE**

Pg 19

**THE ART OF RESILIENCE
INCIDENT MANAGEMENT
MASTERY**

Pg 20

**HOW DUE DILIGENCE
CAN MINIMIZE SUPPLY
CHAIN RISKS**

Pg 23

**IS ARTIFICIAL INTELLIGENCE
A FOE OR A FRIEND?**

Pg 28

**PROTECTING THE SCADA
NETWORK**

Pg 30

**THE NEED FOR ALTERNATIVE
INVESTMENTS: NAVIGATING
THE PATH TO FINANCIAL
SUCCESS**

Pg 32

**EMPOWERING SMALL
BUSINESSES: THE IMPERATIVE
OF COMPUTERIZED ACCOUNTING
SYSTEMS IN MANAGING RISK**

Pg 34

**PROTRACTED REFUGEE
SITUATION: CAUSES,
CHALLENGES & SOLUTIONS**

Pg 38

**THE GOOD, THE BAD AND
THE UGLY OF HIRING HIGHLY
TALENTED PEOPLE**

Pg 40

**THE PERILS OF LIVING ABOVE
YOUR MEANS: NAVIGATING THE
FINANCIAL TIGHTROPE**

Pg 43

**MANAGING LEGAL &
COMPLIANCE RISKS IN
BUSINESS: THE IMPERATIVE
OF SEEKING LEGAL COUNSEL**

Pg 45

**HOW IS THE HYGIENE OF YOUR
PERSONALLY IDENTIFIABLE
INFORMATION (PII)?**

Pg 47

**ENTERPRISE RISK MANAGEMENT
IN A DIGITAL SPACE**

Pg 50

PUZZLE ISSUE NO.8



MILTON STEVEN OWOR

The Chief People & Culture Officer - NSSF

Shares his views on contemporary human resources management practices.

Qn1: Briefly tell us who Milton is and your role at the National Social Security Fund (NSSF)

My name is Milton Steven Owor, born several years ago in Rubongi, Tororo, in Eastern Uganda. I am happily married to Betty for the last 26 years, and together we've been blessed with 3 children: Adrian, Phoebe and Michelle.

I hold a BA (Economics and Social Administration) from Makerere University, MBA (University of Leicester, UK) and Certification in Business Management (INSEAD, France). I am a professional Executive Coach, practicing at Advanced Level, and a member of the International Coaching Federation.

At the Fund, I work as the Chief People & Culture Officer (CPCO), a role I have held since February 2017. As CPCO, my role is to ensure that the Fund has the right talent, at the right time and at the right cost.



Qn2: What is the role of HR management in shaping the strategic direction of an organisation?

The strategic direction of an organisation refers to the long-term goals and objectives that guide its decisions and actions. HR management contributes to this process in several ways:

Workforce planning

Workforce planning ensures that the organization has the right people with the right skills at the right time. HR managers assess the current and future workforce needs of the organization. They identify the skills and talents required to achieve the strategic objectives.

Talent acquisition and retention

HR is responsible for recruiting, selecting, and onboarding employees who align with the organization's strategic goals. It also develops and executes effective retention strategies to ensure that the organization retains key talent and knowledge critical to the delivery of its strategic plan.

Training and development

HR designs and implements training programs to develop employees' skills and competencies in line with the organization's strategic objectives. Continuous learning and development help employees adapt to changes in the business environment and contribute effectively to strategic initiatives.

Performance Management

HR establishes performance metrics and evaluation processes to align individual and team performance with organizational goals. Performance management systems

help identify high performers, address underperformance, and ensure that employees' efforts contribute to strategic outcomes.

Leadership development

HR identifies and develops leadership talent to ensure that the organization has capable leaders who can implement the strategic vision. Succession planning is a key aspect of leadership development, ensuring a pipeline of leaders ready to take on key roles.

Culture and organizational values

HR plays a key role in shaping and reinforcing the organizational culture that supports the strategic direction. Aligning the values, beliefs, and behaviors of staff with the strategic goals of the organization helps create a cohesive, engaged and motivated workforce.

Qn3: What are the emerging trends for hiring human resources in the contemporary world?

Remote work and virtual hiring

The Covid-19 pandemic accelerated the adoption of remote working. Virtual hiring processes, including video interviews and remote onboarding, have become a lot more prevalent. Even as the pandemic recedes, many organizations, the NSSF inclusive, continue to offer remote work options.

Artificial intelligence (AI) and automation

AI and automation tools are being increasingly used in the hiring process to streamline tasks such as resume screening, candidate sourcing, and initial assessments. These technologies significantly enhance efficiency and reduce bias in the hiring process.



Data-driven decision-making

HR analytics and data-driven decision-making are gaining importance. HR professionals are leveraging data to assess the effectiveness of recruitment strategies, employee engagement initiatives, and overall HR practices.

Focus on diversity, equity, and inclusion (DEI)

Organizations are placing a greater emphasis on creating diverse, equitable, and inclusive workplaces. The benefits of DEI to organizations are massive, including higher innovation, staff engagement, productivity, brand equity, profitability, among others.

Candidate experience and employer branding

Improving the candidate experience has become a priority for organizations. HR teams are focusing on creating positive impressions from the initial application through the entire hiring process. A strong employer brand is crucial in attracting top talent.

Upskilling and reskilling

Given the rapid pace of technological change, HR is playing a key role in identifying skills gaps and implementing upskilling and reskilling programs. Continuous learning and development are becoming integral to talent management strategies.

We strongly believe in supporting staff development and growth. To this end, we have recently launched Pathfinder, our cutting-edge career development initiative. Pathfinder enables our staff to listen to and engage with professionals who have walked the journey and excelled in their various areas and career paths.

Through these engagements, our staff can pick practical ideas and energy to enable them to walk their own journey with more competence, confidence and self-belief.

Flexible work arrangements

Flexibility in work arrangements, including hybrid models (Office and remote working), is a significant trend, contributing to a better work-life balance. At the Fund, we have implemented a 3-2-2 policy (3 days work from the office, 2 days from home, and 2 weekend days), which has worked so very well for us in the last 3 years. Our productivity, staff engagement, employer brand attractiveness, have all continued to rise.

Employee well-being

Employee wellness is the overall well-being of an individual employee or group of employees. It encompasses both physical and mental health and well-being.

Organizations are recognizing the importance of employee overall well-being, because of its significant impact on organizational performance. At the Fund, we have various wellness programs, including our annual Step Challenge (this year 2023 we walked to Paris!), Counselling services

including mental health, gym services for all staff, creche for our new mothers, healthy eating habits for staff and their families, regular medical checkups, Company Health Advisory, among many others.

Qn4: Employees come from diverse cultural backgrounds. How do you manage to build a coherent organizational culture?

Building a coherent organizational culture in the context of a diverse workforce requires intentional efforts to foster inclusivity, respect, and shared values. Here are some strategies we leverage to manage and build a coherent organizational culture in the context of diverse cultural backgrounds:

Define core values

We have clearly defined and communicated the core values that represent the Fund. Our core values, which are published and are well understood by all our staff and customers are; Customer Centricity, Innovation, Integrity, Teamwork and Efficiency. These values are inclusive and resonate with employees from all cultural backgrounds. All our staff are committed to ensure that in all that they do, they remain consistent with the Fund values.

The Fund values also align with the overall mission and goals of the Fund.

Inclusive leadership

We strive to foster inclusive leadership at all levels of the organization. Our Leaders are coached to actively promote diversity and inclusion, listen to different perspectives, and model behaviors that value and respect individuals regardless of their cultural background. Through our annual 360-degree assessments, our leaders obtain critical feedback on their leadership and alignment to Fund values. All our leaders are required to act on the feedback given, so that they can consistently improve on their leadership abilities.

Psychological safety and open communication

We encourage open and transparent communication. We create channels for employees to share their thoughts, ideas, and concerns. We strive to ensure that everyone has an equal opportunity to voice their opinions without fear of retribution, and actively listen to diverse perspectives. Through the quarterly MD Townhalls, departmental meetings, whistleblower platform among others, each staff has an opportunity to engage with everyone else in the organization, including the most senior leaders.

Celebrate diversity

We actively celebrate and acknowledge cultural diversity within the Fund. This includes recognizing religious holidays, organizing events that highlight different traditions, and incorporating diverse perspectives into company communications and materials.

Establish inclusive policies

We regularly review and update our HR policies to ensure they are inclusive and considerate of diverse cultural needs. This includes flexible work arrangements, religious accommodations, gender sensitivities, and other policies that support a diverse workforce. Such policy shifts include the introduction of a Creche at head office, to allow our new mothers bring their newborns at work, so that they can attend to them, especially breastfeeding, while at work.

We ensure that organizational leaders, starting with the Managing Director and EXCO, are committed to diversity and inclusion initiatives.

Cross-cultural teams

We create cross-cultural teams that leverage the strengths of individuals from different backgrounds. This allows employees to learn from one another, share experiences, and develop a deeper understanding of diverse perspectives.

Mentorship and buddy programs

We introduced mentorship and buddy programs that pair employees from different cultural backgrounds. This helps newcomers integrate into the organization, understand the company culture, and build connections with colleagues.

Address unconscious bias

We provide training and resources to address unconscious bias in the workplace. This helps employees recognize and mitigate biases that may impact decision-making, hiring processes, and interactions with colleagues.

Regular culture assessments

We conduct regular assessments of the organizational culture to gauge how well it aligns with the desired values. Feedback from our staff helps to identify areas of strength and areas that need improvement.

Qn5: Attraction and retention of critical talent is a big problem for most organizations. How do you address this in the NSSF?

We recognize the importance of critical talent to the achievement of the organization's goals and objectives, and we, therefore, develop appropriate programs to attract and retain talent, as explained below:

Employer branding

The Fund has developed a strong and positive brand that communicates the mission, values, and benefits of working at the NSSF. Our culture, underpinned by our values, makes us attractive to high potential hires, including from leading blue chip multinational companies. Our initiatives, such as the Hi-Innovator program, that is creating value to the communities, further drives our employer brand attractiveness.

Strategic recruitment

The Fund conducts targeted and strategic recruitment to attract individuals with the unique skills and expertise required for critical roles within the organization. This sometimes involves partnerships with educational institutions through our Graduate trainee program, industry associations, or targeted advertising.

Competitive compensation

We offer competitive and fair compensation packages that align with industry standards, the Ugandan market, and the unique demands of specific roles. We also consider additional benefits such as health and wellness programs, and staff retirement plans (Staff Provident Fund).

Professional development

We emphasize professional development opportunities to attract individuals who are committed to continuous learning. This includes training programs, workshops, and opportunities for skill enhancement. We have a world-class, cutting-edge e-learning platform, Percipio, through which our staff access 3000+ on-line courses, offered by the world's leading Universities. These are conveniently accessed via audio, visual (videos), and text. So, even while in the traffic jam, our staff can plug in and listen to educative material and watch the various learning videos.

Flexible work arrangements

Like I said earlier, we offer flexible work arrangements, such as remote work options or flexible scheduling, to accommodate the diverse needs and preferences of our staff. Our 3-2-2 work plan policy helps us deliver this flexibility.

Qn6: What are the major HR challenges that the NSSF faces and how do you address them?

Despite the tremendous progress we have made in building a competent, motivated, and engaged workforce, we continue to experience several challenges, including but not limited to:

Talent acquisition

There is limited exceptional talent in the market, especially for the specialized areas of our industry i.e., pension management. There is also skill shortage in areas like AI, Data Science, Software development, Data Analytics. To mitigate this, we focus on talent mapping (knowing who is in the market), upskilling internal talent, and growing our own future talent pipeline through our Graduate Training program.

Multi-generational workforce

Maintaining high levels of employee engagement is a challenge because of the multi-generation nature of our workforce, with differing motivation levers.

To address this, we conduct regular employee engagement and pulse surveys, to help us identify the drivers and barriers to employee engagement. The objective is to eliminate the barriers, while enhancing the drivers of employee engagement through reward and recognition.

Cost of employee well-being

To achieve employee well-being requires a significant resource envelop, which may sometimes not be readily available. Nonetheless, addressing employee overall well-being remains a priority area for us. We have just gone through the traumatic experience of Covid-19 pandemic, where many staff lost their loved ones. The Fund has offered wellness programs, including but not limited to physical and mental health support.

Qn7: As an HR practitioner, how do you see the role of HR in the changing work environment?

The role of Human Resources (HR) is evolving in response to the changing work environment.

Firstly, an HR Manager needs to continuously analyze the environment to be able to know the current and future trends in human resource management. Most importantly, the HR Manager needs to analyze the following questions and provide appropriate responses:

- What is changing?
- What is driving the change (Technology- AI, Machine Learning, Robotics, Data science, etc., demographics, climate change, etc.)
- How are the changes likely to impact the organizations?
- Where are we in relation to the change(s)?

Secondly, the HR Manager needs to determine strategies on how to prepare the workforce to respond appropriately to the changing business environment. That means the contemporary HR Manager needs to be up to date with current developments, have a good sense of foresight, be analytical and strategic.

The changing work environment requires HR practitioners to be agile, strategic, and adaptable. The focus is on creating a positive employee experience, leveraging technology, and aligning HR practices with the organization's strategic goals to drive business success in a dynamic and evolving landscape.

Qn8: The NSSF is a technology-driven organization, with high levels of automation. How do you ensure job security for staff vis a vis the high level of automation?

It is indeed true that we are a highly technology - driven organization and the automations are all aimed at enhancing efficiency and delivering convenience and a better experience to our members, customers and staff.

That notwithstanding, we still value human interaction and there is still a large room for human input, especially in discernment and cognitive space, where technology is still limited.

Qn9: The NSSF is one of the best performing government entities in the country. How are you able to achieve this amid the bureaucratic bottlenecks associated with government entities?

The Fund's strong performance is anchored on several factors:



The first one is having a clear and stretched strategy that is understood and embraced by all staff, at all levels. Every one of us understands the Fund's vision 2025, and our individual role in achieving it.

Secondly, we ensure that every staff member has absolute clarity on the performance expectations of them for the year and are given the necessary tools and leadership support needed to deliver the results. This is reinforced by an equitable performance-driven reward framework.

Finally, the above succeed because we have full support and commitment from senior management, the Board and our political leadership, notably, the Minister of Gender, Labour and Social Development as well the Minister of Finance, Planning & Economic Development.

Qn10: What is your philosophy on work-life balance, and how does it inform your NSSF HR policies?

I believe that the most productive and happy staff are those that have their work-life balance equation right. And the 'right balance' differs for every employee, depending on their prevailing personal circumstances. It is for every leader to ensure they remain adequately 'connected and in tune' with their staff, so that they can appropriately support staff to attain this balance, without compromising the Fund's objectives.

Qn11: Can you share examples of your HR initiatives that have had a positive impact on the Fund's culture and employee satisfaction?

We have had many initiatives aimed at driving Fund culture and employee satisfaction. These are all embedded in our HR strategy. Some examples are listed below:

i) Competitive reward framework

Competitive reward framework, driven by performance. 70/30 strategy on variable pay, delivers superior performance.

ii) Employee wellness

Robust wellness programme, including gym for all, creche, counselling services, mental health, Company Health Advisory, etc., have had a positive impact on the employee satisfaction levels.

iii) People development

People development- Investing in robust e-learning platform (Percipio), Pathfinder, coaching mindset, 80:20 resourcing strategy to encourage growth of inhouse talent, coaching and mentoring for leaders, have enhanced employee satisfaction.

iv) Employee engagement

Open communication is strongly encouraged at the Fund. Through employee engagement surveys + pulse survey, and 360-degree feedback mechanisms, as well as the MD's quarterly townhalls, staff can communicate any matter to their supervisors and colleagues. The leaders always ensure that all the issues raised by the staff are resolved, which makes the staff feel respected.

Qn12: Any other message you would like to share with our readers?

I would like to leave the readers with the following quotes:



Take care of your employees, so they will take care of your business. It is as simple as that.

– Sir Richard Branson –



Train people well enough so they can leave, treat them well enough so they don't want to.

– Sir Richard Branson –



BOSS UP

Take your **business** to the next level.

Sign up for the free online **NSSF Hi-Innovator Business Academy**, upskill yourself and stand a chance to win up to **UGX 75,000,000** in seed funding.

Business development services support | Innovation ecosystem networks access to business mentorship | Referrals to potential investors at scale

Visit hi-innovatorbusinessacademy.nssfug.org or call 0392000152 for more information.

*T&Cs apply.



Implemented by



In partnership with





2023: A YEAR IN REVIEW

NICKSON AHABWE

Risk Management Practitioner

A pulse check

8 Risk Management lessons from 2023 through the lenses of an ERM practitioner.

The manifestation of the global health pandemic and subsequent geoeconomic confrontations in recent years have been a thorny reminder to both businesses and other organizations, of the importance of Enterprise Risk Management (ERM). As such, risk management experts continue to be on demand as entities seek to proactively determine how to best plan for and cope with the impacts of unforeseen circumstances.

Is your entity prepared to tackle what lies ahead and can it withstand the next shock? The answer lies in your level of preparedness. The more prepared you are, the more appropriately you can respond to emerging risks.

Speaking of preparedness, one doesn't have to look far to get pertinent insights and lessons to start the journey, considering that risk and opportunity management are part and parcel of everyday life.

Let's explore and learn from a selection of memorable events of 2023 (focus on Uganda but with a global fusion), highlighting a range of constant risks that may continue to shape the risk landscape over the coming years.

Financial Risks

Volatile financial environment: The Case of Silicon Valley Bank

Silicon Valley Bank (SVB), the 16th largest U.S. bank before its collapse, was shut down in March 2023 by the California Department of Financial Protection and Innovation, according to an article by Erin Globler on Investopedia. The bank was shut down after its investments greatly decreased in value and its depositors withdrew large amounts of money, among other factors. SVB didn't have sufficient cash on hand to meet its depositors' cash withdrawal demands, because cash was tied up in long term investments.

Consequently, they started selling their bonds at a significant loss, which caused distress to customers and investors. A classic case of asset-liability mismatch!



Silicon Valley Bank collapse, 2023

MARCH 8: Silicon Valley Bank (SVB) announces \$1.75 billion capital fundraising.

MARCH 9: SVB stocks plummet by 60%.

MARCH 10: SVB collapses after a bank run fueled by social media. Government regulators take over the bank.

MARCH 12: U.S. government announces it will guarantee all deposits at SVB.

MARCH 13: HSBC buys U.K. arm of SVB.

MARCH 14: Moody's Investor Service adds six regional banks to the review list for credit rating downgrades.

MARCH 17: SVB Financial Group, Silicon Valley Bank's former parent company, files for Chapter 11 bankruptcy protection.

MARCH 26: First Citizens Bank buys Silicon Valley Bank.

In its Annual Report for 2023, Bank of Uganda (BOU) noted that financial risks remained elevated due to the fragile risk environment, largely attributed to three major global developments, namely, (1) The geopolitical tension and conflict in Ukraine, (2) Fiscal and monetary contradictions in the United Kingdom and (3) a banking crisis in the US, which saw a failure of two major banks, SVB and Signature Bank.

To manage the elevated financial risks, BOU revised the risk limits during the year, among other measures.

Risk lesson 1: Risk is not static

Continuously reassess risk management practices. Risks tend to linger in obscure and unexpected places. So, even in good times, things can go suddenly and terribly wrong if you don't practice effective risk management that considers all possible scenarios.

Reputation Risks

a) NSSF Probe

In February 2023, the Parliament of Uganda investigated the operations of the National Social Security Fund (NSSF), with the Parliament's select committee eventually giving 27 recommendations.

LIVE: NSSF probe chair presents final report in parliament

1 Mar 2023 - MP Mwine Mpaka, the committee chairperson, read his findings and recommendations in front of a packed house.

With the proceedings of the probe telecast live, highlights shared on social media as well as making headlines in the national newspapers, NSSF found itself at the center of every conversation in the country. The tonality line of its brand was clearly thin and blurred at the time, oscillating between a positive and a negative depending on who you talked to.

In the Annual Integrated Report for 2023 released in September, the Fund reported a decline in the tonality score from 95% in 2022 to 79%, although this subsequently bounced back to 95% in May 2023. Reputation risk was also highlighted in the embedded risk management report with a significant increase in rating from green in FY21/22 to a red in FY22/23.

Withering this storm is perhaps a testament of resilience of the NSSF brand.

If one is to hold a deep conversation with one of NSSF's top brass (my pick is on the Chief Risk Officer), they would surely walk away with invaluable lessons on how to develop and maintain a thick skin during turbulent times.

b) What is in a name?

In September 2023, Biyinzika Enterprises Limited (BEL) had some of its properties advertised for sale by a hired Kampala based law firm on behalf of a lending bank, according to the New Vision, a local newspaper of September 12, 2023.

Due to similarities in the brand names, concerned shareholders of Biyinzika Poultry International Limited (BPIL), a totally different company but with a similar name, immediately sought answers from their fiduciary management team. To clear the brand confusion, BPIL had to dig into their coffers and publish a statement clarifying that BPIL and BEL were separate legal entities.

Clearly, a brand can be delicate and must be protected at all costs.

Risk lesson 2: Reputation is everything, guard it well.



It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.

- Warren Buffett -

Regulatory Compliance Risks

World over, regulatory frameworks provide an enabling environment in which businesses operate to execute their respective mandates. As a win-win governance aspect, the frameworks are also instrumental in the protection of a wide range of stakeholder needs and interests.

a) Enforcement of the data protection and privacy Act, 2019

In June 2023, the Personal Data Protection Office (PDPO), the body responsible for, among others, enforcement of the Act, initiated an investigation into Uganda Securities Exchange (USE) and its software provider Soft-Edge Limited, following a complaint of an alleged breach, where personal information belonging to users of the USE was illegally accessed.

The PDPO issued its report, (Abridged Investigation Report of the Data Security Breach at Uganda Securities Exchange [USE], June 2023), detailing its findings, which included among others, the confirmation of personal data security breach for 12 days without the knowledge of either the USE or Soft-Edge Limited. Subsequently, both parties were given a three-month period within which to rectify all areas of non-compliance identified.

b) The Petroleum Authority of Uganda temporarily halts work at the Kingfisher Oil project

According to The Observer, a Ugandan weekly newspaper of October 7, 2023, Uganda's petroleum regulator suspended work at CNOOC'S Kingfisher oil project area after a fatal incident.



"This regrettable incident follows several safety incidents previously brought to the attention of CNOOC Uganda Limited. This trend is unacceptable as it compromises the safety of the personnel and damages the safety of the sector," the Petroleum Authority of Uganda said in a letter (PAU 10/01/002) to CNOOC Uganda.

Risk lesson 3: Comply or pay, albeit heftily!

The risks of non-compliance are not only limited to the heavy fines that could be imposed but extend to license withdrawal and reputational risk, which could have dire consequences.

It is, therefore, important for entities to be on the right side of regulation, by having a compliance team and systems to monitor and enforce regulatory requirements.

Cyber Risks

In the World Economic Forum's - Global Risks Report 2023, Widespread cybercrime and cyber insecurity is ranked among the top 10 global risks, both in the short and long term (a 2-year and 10-year period). With the technological evolution and increasing automation, the report notes that technology will exacerbate inequalities while risks from cybersecurity will remain a constant concern and increasingly sophisticated, targeting sensitive data.

Hackers shake Kenya's digital financial system



In July 2023, the Business Daily Africa reported that a major cyber-attack caused an outage of more than 5,000 public services in Kenya for more than 48 hours, while disabling internet-based and mobile payment platforms.

This incident brought back memories of a similar attack in Uganda that happened in August 2022. At the time, hackers infiltrated the National Water and Sewerage Corporation (NWSC), a national water utility's IT system, which disabled and almost crippled some of its operations, according to a local newspaper, the Daily Monitor of August 25, 2023.

In their recent IPO prospectus, both Airtel Uganda and MTN Uganda, listed security breaches or cyber-attacks as part of the material risks to their operations.

A winning bet is that if one is to access all corporate reports within the country or world at large, one would find that cybersecurity risk is a common feature on their risk registers.

Risk lesson 4: No one is immune from cyber attack - Invest in cybersecurity measures.

There are no sustainable shortcuts to the management of this risk. Every institution can be attacked at any one moment and, therefore, each institution must continuously develop robust cyber risk mitigation strategies.

ESG Risks

a) Environmental Risks

Floods and landslides are some of the common-climate change-related effects that keep recurring in Uganda. The impacts are huge, with lives and livelihoods often lost, not forgetting the cost of replacing the infrastructure. In May 2023, torrential rains swept away the Katonga bridge on the Kampala- Masaka highway.



This is a global dilemma and Uganda is not alone. In September, 2023, heavy rainfall led to flooding across portions of the New York metropolitan area in United States.

The Institute of Risk Management periodically issues guidance on what Risk Managers could do in helping to address the climate crisis. In its recent publication Enterprise Risk Autumn 2023, learnings from disasters like earthquakes, floods and hurricanes are featured. Key to note is the requirement to conduct a realistic risk assessment to understand how critical infrastructure will perform during a disaster as part of the business continuity plan, is an imperative.

Risk lesson 5: Risk of environmental disaster has heightened- Support ESG initiatives

What remains clear is the fact that we are all affected by environmental risks and thus we must play a collaborative role to manage this global risk.

b) Social Risks

i) Safety Risks

A quick google search about Uganda in 2023 (https://en.wikipedia.org/wiki/2023_in_Uganda) returns damning safety related results. Of the 17 results returned at the time of penning this article, 76% were safety related with the remaining 24% about the Anti-Homosexuality Bill.

The above statistics include nine lives that were lost due to a stampede at a music show at Freedom City mall, in Najjanankumbi, a suburb of Kampala city, the so many lives

lost in traffic accidents, the ADF attacks that led to the death of 38 students and injuries to several others when the ADF attacked Lhubiriha Secondary school in Mpondwe, Kasese district in June 2023, as well as the recent attack that led to the death of two foreign tourists and their local driver in Queen Elizabeth national park.

Unfortunately, the above statistics are not all-inclusive of safety incidents that occurred in the country.

Risk lesson 6: Safety risk is imminent

Develop a well-designed and comprehensive safety management system/culture. Life is irreplaceable!

ii) Social Activism Risks

Use of social media has promoted social activism; it does not only provide a channel for instant messaging, but the images shared on social media can arouse strong emotions, which help to galvanize support for a particular cause. During the year 2023, a number of hashtags dominated our feeds, the most prominent one being the (#Kampalapotholeexhibition), which displayed pictures of various deep potholes around Kampala, forcing Kampala Capital City Authority to announce a plan for patching up various potholes in the city.



Risk lesson 7: Your brand is one post away from being tested for its resilience!

Having an active social media presence for corporate institutions is no longer a luxury but rather a must have.

c) Governance Risks

i) Lifting the corporate veil: Director's personal liability

Section 20 of The Companies Act, 2012 empowers courts to lift the "corporate veil" when there is evidence to show that the corporate structure was used purposely to avoid or conceal liability." When the corporate veil is lifted, directors and shareholders can be personally held liable for the company's actions.

In a judgement delivered by Hon Justice Stephen Mubiru on the 19th of September 2023, the High Court of Uganda, in the case of Absa Bank of Uganda Limited v Enjoy Uganda Limited (Miscellaneous Application 1243 of 2023), ruled that the corporate veil can also be lifted in cases of wrongful or fraudulent trading. Fraudulent trading is a premeditated act, committed with the intention of defrauding creditors, while wrongful trading occurs when the company continues to trade and run up debts when knowingly insolvent, but there is no proven dishonesty or malicious intent involved.

In this case, two directors of Enjoy Uganda Limited were held liable for the loan obligations in default.

ii) Perceived potential conflict of interest: Resignation of the BBC Chairperson

The Institute of Corporate Governance in Uganda lists impartiality as one of the five principles of corporate governance. The other four are responsibility, accountability, risk awareness and transparency.

Under impartiality, boards and directors are expected to approach every decision with an independent mindset, ensuring no personal interests or those of close colleagues come between them and business decision.

In April 2023, the Chairman of the British Broadcasting Corporation (BBC), Richard Sharp, resigned after an investigations report found that he failed to disclose a potential perceived conflict of interest arising from his involvement in facilitating a loan of almost \$1 million to former British Prime Minister Boris Johnson.

"There may well have been a risk of a perception that Mr. Sharp would not be independent from the former Prime Minister, if appointed," the report said.

Risk lesson 8: Transparency and ethical business conduct are important principles of good corporate governance.

The board of directors must exercise prudence and diligence in their roles to avoid personal liability and to ensure the rights and interests of stakeholders are always safeguarded.

2024 Global risk outlook

Looking at publications from various players (Institute of Internal Auditors, Economist Intelligence Unit, World Economic Forum, etc.), there are common themes for the global risks outlook for 2024.

Modest global growth is expected in 2024, continued monetary tightening, supply chain disruptions, digital disruption and the advent of new technologies, persistent environmental threats and geopolitical conflict could weigh heavily on the global economy in the year 2024.

Focusing on Uganda, a few factors have caught my eye in relation to the heightening of the investment risks.

In summary,

- BOU notes that the prospects of domestic economic growth continue to be impacted by adverse global economic developments, tighter domestic monetary and financial conditions as well as falling consumer and business confidence.
- The World Bank Group issued a statement in August 2023 suspending new public financing to Uganda following the enactment of the Anti-Homosexuality Act, 2023. World Bank is a major financier across various sectors in Uganda, thus this decision has far-reaching implications. The Government of Uganda is still engaging the World Bank on this matter.

- In October 2023, the US Government issued a Business Advisory on Uganda, informing U.S nationals of potential financial and reputational risks resulting from what they described as endemic corruption, weak rule of law, bureaucratic delays and an increasingly aggressive tax collection regime, among other risk factors, that they (US nationals) may face while conducting business in Uganda.

However, it is important to note that in a detailed 2023 Investment Climate Statement (by the US Government), Uganda is considered a welcoming country, with a free-market economy and liberal financial system.

Final thought

By taking time to reflect on the rollercoaster 2023 has been, we arm ourselves with valuable insights to be better equipped to face the years ahead.

The operating landscape continues to be volatile, which calls for proactive risk management. As drawn from the 2023 events, financial dynamics, brand index, heightening regulatory regime, technological advancement, ESG issues and the associated challenges, are some of the critical risk drivers that Risk Managers need to continue to focus on in the years to come.



CYBER EXTORTION

NAVIGATING A RISING THREAT LANDSCAPE

NORBERT NAMANYA

Information Security Specialist - NSSF



In the contemporary digital era, organizations and individuals find themselves grappling with an escalating and hazardous facet of cybercrime—cyber extortion. This disreputable practice involves threat actors demanding payment or specific actions, leveraging the threat of exposing sensitive information, compromising data integrity, or disrupting critical business operations through denial of service (DoS).

Cyber extortion serves as an overarching term encompassing various forms of digital blackmail, including ransomware attacks, Distributed Denial of Service (DDoS) attacks, doxing (Online harassment) and sextortion.

This article digs into the proliferating trend of cyber extortion, spotlighting a particularly concerning variant—sextortion. Derived from “sex” and “extortion,” sextortion unveils a covert form of cyber threat that leverages compromising or explicit personal content to coerce individuals into submission to malicious demands. In the realm of cybercrime, it serves as a malicious tool wielded by cyber extortionists seeking financial gain or other immoral objectives. Sextortion goes beyond the mere invasion of privacy; it strategically exploits personal weaknesses to manipulate and control victims. Understanding the shades of this evolving threat is paramount, as we navigate the intricate landscape of cybersecurity.

Let's explore sextortion manifestations, impact, and most importantly, strategies for individual empowerment and defence against its crafty reach.

Unlike traditional forms of cyber extortion, sextortion primarily targets individuals within corporate environments, capitalizing on their high personal reputation derived from their positions, family backgrounds, or institutional affiliations. Cybercriminals employ unscrupulous tactics to extort money by collecting highly sensitive personal information and threatening to disclose it if their demands are not met. To illustrate this phenomenon, let's imagine a harrowing experience of an individual—call him Smith.

Smith, a regular corporate worker, encounters a shocking email in his inbox one Monday morning. An anonymous sender claims possession of compromising photos and videos, allegedly capturing Smith in inappropriate activities at the workplace, potentially through compromised office surveillance cameras. The extortionist threatens to release

this material unless a significant sum is paid to a specified cryptocurrency address within a short timeframe. Adding to the menace, the sender asserts access to sensitive corporate data that Smith is responsible for, intensifying the potential impact on both the individual and the organization he represents.

In our interconnected digital landscape, such scenarios are likely to persist, necessitating vigilance and precaution to mitigate potential risks. This form of online extortion involves threat actors exploiting compromising information to coerce victims into submission.

Even within corporate environments, individuals are not immune, facing threats ranging from personal content exposure to the divulgence of sensitive corporate data. Faced with such a situation, maintaining composure is paramount; victims should resist the urge to comply with extortion demands, as payment often exacerbates the issue. Swift action is crucial when dealing with cyber extortion. Victims should document all communication, report incidents to IT and security teams, involve law enforcement when criminal activities are suspected, and seek legal advice for potential remedy. Simultaneously, notifying the human resources department or management, ensures that the organization is made aware of the risks and can take steps to secure its systems, if the demands transcend personal information to organizational data.

Transparency within the workplace, without divulging sensitive details, helps colleagues remain vigilant, fostering a collective defence against future cyber threats.

Preventing sextortion goes beyond technological defences; it requires individuals to fortify their own cyber defences through a combination of awareness, integrity, and responsible digital practices. At the workplace, being cognizant of organizational policies against engaging in inappropriate behaviour is crucial. By adhering to these guidelines, individuals can significantly reduce the likelihood of falling victim to sextortion schemes that exploit compromising situations.

Moreover, fostering a culture of integrity, where individuals consistently choose to do the right thing, even when no one is watching, serves as a powerful deterrent against potential extortionists.

In addition to awareness, individuals must be vigilant about the information they store on organization computers such as personal photographs, videos from personal occasions, as these can be soft points for attack. Avoiding the storage of personal and confidential information in the workplace environment minimizes the ammunition available to potential cyber attackers. By treating company resources with respect and using them exclusively for work-related activities, employees can create a digital environment less susceptible to exploitation. This heightened sense of responsibility not only safeguards personal dignity but also contributes to a collective defence against the ever-evolving landscape of cyber threats.

Ultimately, the individual's role in mitigating sextortion is paramount. By staying informed, practicing integrity, and adopting responsible digital behaviours, each person becomes an active participant in building a resilient defence against the invasive reach of cyber extortion. As we navigate the complexities of the digital age, personal commitment to cybersecurity emerges as a formidable shield, protecting against the sinister threats posed by sextortion.

Organizations must now, more than ever before, enhance their cyber security awareness programs, focusing on trending data breaches occasioned by cyber-threat actors, locally and internationally. Organization/individuals should enhance personal cybersecurity measures and limit exposure, update passwords, and enable a two-factor authentication to curb the vice.

Crafting a public relations strategy is vital to managing organizational reputational damage. Finally, creating a resilient cybersecurity culture through employee training remains a proactive defence against the evolving cyber threat landscape.

Following these guidelines enables potential victims to navigate the challenges of cyber extortion while safeguarding personal dignity and corporate integrity.

The decision to pay or not in the face of a cyber extortion attack is complex, loaded with financial, ethical and regulatory implications. In some cases, the regulator may impose a penalty against an institution that pays a ransom, because the regulator considers it as an act of promoting crime.

Additionally, payment of a ransom doesn't guarantee data restoration, or not releasing explicit material in possession and victims might become more attractive targets for future attacks. However, for some, paying the ransom might seem the quickest way to restore operations, considering potential costs of downtime, data loss, reputational damage, and regulatory penalties. Organizations must weigh the options, ideally with the guidance of cybersecurity professionals and law enforcement agencies.

The role of cyber insurance in mitigating the financial impact of a cyber-attack, including ransom payments, is a pertinent consideration. It offsets recovery costs, legal fees, and incident response expenses. However, organizations must navigate the complexities of insurance policies, as coverage and costs vary based on factors like industry, size, and risk categories. While cyber insurance offers a haven for cyber-losses in terms of paying insurance proceeds for loss suffered, it is important to have a thorough understanding of policy coverage, as some aspects and circumstances may not be covered.

In conclusion, as cyber extortion continues to evolve, organizations and individuals must remain vigilant, adopt proactive measures, and foster a culture of cybersecurity resilience. By understanding the intricacies of cyber threats, making informed decisions, and implementing robust preventive strategies, they can navigate the dynamic landscape and protect themselves against the multifaceted challenges posed by cyber extortion.



SHAPING YOUR FINANCIAL FUTURE

THE ART OF STRATEGIC ASSET ALLOCATION

MICHAEL SENDIWALA

Senior Manager, Investment Risk - NSSF



For many people, when making investment decisions, the focus is on return, and little attention is paid to the associated risks. It is common to see people rushing to invest in any venture that promises a high return, ignoring the fundamental principle of investment, which is, the higher the return, the higher the risk. Recently, Capital Chicken, a ponzi scheme, promised a return of 40% for a 5-month investment. Several people invested their funds in the scheme, which closed shop after a few months before investors could recover their principal and interest - the estimated loss was UGX2bn.

However, savvy investors understand that the key to building long-term wealth is not in market timing or stock-picking prowess but in a well-thought-out strategy known as strategic asset allocation. This article delves into the concept of strategic asset allocation, its importance, the risks to pay attention to and how to master this art to achieve your financial goals.

Strategic asset allocation (SAA) is a disciplined and long-term investment strategy that involves the allocation of your investment funds across different asset classes, such as stocks, bonds, real estate and cash. The goal is to achieve a balance between risk and return, aligning your investments with your financial goals and risk tolerance.

The process of asset allocation involves:

- a. **Identifying financial goals:** Begin by clearly defining your financial goals. Whether it's retirement planning, buying a home, funding your children's education, or simply building wealth, your objectives will dictate your allocation strategy.
- b. **Risk appetite:** Understanding your risk tolerance is crucial. Are you comfortable with potential volatility of the stock market, or do you prefer a more conservative approach? Your risk appetite will help determine the asset mix that suits you best.
- c. **Selecting asset classes:** Each asset class has distinct risk and return characteristics. Equities offer growth

potential but come with higher volatility. Bonds provide stable income but may offer lower long-term returns. Real assets like real estate and commodities can be a hedge against inflation. Cash equivalents offer safety but typically have limited growth.

- d. **Allocation percentages:** Based on your goals and risk tolerance, determine the percentage allocation to each asset class. For example, a young investor with a long-time horizon may allocate a larger portion to equities, while someone approaching retirement might opt for a more conservative mix, with a higher bond allocation.

Below, are key risks that an individual or entity must consider as they develop their SAA:

- i. **Concentration risk:** This risk arises when a significant portion of an individual's assets, investments, or revenue is concentrated in a particular area. If that area experiences adverse developments, it can lead to substantial losses or financial instability.
- ii. **Inflation risk:** Is the risk that the real value of an investment or cash will erode over time because of inflation. Inflation is the increase in general price level of goods and services in an economy, leading to a decrease in purchasing power of a currency. For instance, if you are a long-term investor, there is a possibility that the value of your investment could be eroded due to increase in prices (inflation). Therefore, the expected return should be over and above the expected inflation.
- iii. **Behavioral risks:** Investors may be prone to behavioral biases, such as endowment bias of failing to liquidate a residential house occupied by the owner because of sentimental attachment, yet it accounts for about 90% of a person's wealth, for example. The better choice could be to sell the house and build a cheaper one to get extra cash for investment or retirement planning.
- iv. **Liquidity risk:** Is a critical concept in investing, often considered one of the key risks with certain assets or investment strategies. It pertains to the potential

difficulty of buying or selling an asset in the market without significantly affecting its price.

Imagine the stress you will experience in trying to sell a piece of land to finance a medical emergency! In most cases the land will need to be discounted by almost 50% to get quick liquidity.

So, it is advisable that you do not allocate all your funds to illiquid assets only; your short-term goals should be financed by short term investments.

- v. Economic and geopolitical events:** Certain economic and geopolitical events play a significant role in shaping the global landscape, resulting in economic and political reforms. These events have far-reaching consequences on SAA, therefore, understanding their impact is essential for investment decisions.

For example, the conflict between Russia and Ukraine has led to a slowdown in the global economic growth due to disruptions in trade, causing escalation in inflation around the globe; for instance, in the USA inflation increased from 4.7% (2021) to 8% (2022).

- vi. Taxation risk:** Taxes affect different asset classes differently. In Uganda, different tax rates apply to different asset classes, for example the interest rate on treasury instruments below 10 years is subject to a 20% final withholding tax and dividends are subject to a 10% withholding tax.

- vii. Interest rate risk:** Is the risk that the value of fixed-income investments will decline when prevailing interest rates increase. It is primarily associated with bonds and other debt securities that have fixed rates and whose market prices move inversely to interest rate.

Understanding, assessing and responding to these risks is essential to ensure success of your investment strategy. Below, I explore how to effectively mitigate the risks associated with strategic asset allocation.

a) Concentration risk

- i. Diversification is a cornerstone of investment risk management; by spreading your investments across various asset classes, industries, regions, etc., you reduce the impact of underperformance of a single investment.
- ii. Regularly review and rebalance your portfolio. When certain assets outperform the benchmarks, there is a temptation to increase the allocation to those assets,

thus increasing concentration risk. Rebalancing ensures your allocation remains aligned with your long-term objectives.

b) Liquidity risk

When incorporating less liquid assets like real estate or private equity in your portfolio, assess your liquidity needs carefully. Understand their redemption terms and potential time horizons for accessing your capital. In addition, keep a cash reserve or highly liquid investments in your portfolio to address unforeseen expenses or liquidity needs without having to sell illiquid assets at unfavorable prices.

c) Inflation risk

Consider allocating a portion of your portfolio to assets that historically perform well during periods of inflation, such as stock, real assets (e.g. real estate or commodities), and inflation-protected securities.

d) Interest rate risk

- i. Portfolio diversification- If your allocation includes bonds, diversify your fixed income investments by maturity and duration to mitigate interest rate risk. Shorter term bonds are less sensitive to interest rate changes than long term bonds.
- ii. Consider floating rate bonds - Floating rate bonds adjust their interest payment with changes in market interest rates, providing a degree of protection against rising rates.

e) Behavioral risks - Staying disciplined

Emotions can lead to impulsive investment decisions. Staying disciplined and adhering to your strategic asset allocation plan is crucial. Regularly remind yourself of your long-term goals and risk tolerance.

In conclusion, strategic asset allocation is a powerful tool that can help you build and preserve wealth over the long term. While it doesn't eliminate risk, it provides a structured approach to managing risk and maximizing returns. By customizing your asset allocation strategy to your unique financial situation and consistently reviewing and adjusting it, you can create a more secure financial future. Remember that consulting a financial advisor can provide valuable guidance in developing and implementing your asset allocation strategy.



HOW TO REINFORCE ANTI-MONEY LAUNDERING COMPLIANCE

JOSHUA KIBIRIGE

AML Manager - NSSF



As businesses in the financial sector navigate the current dynamic environment that involves shifts in market trends, changing customer preferences, increasing competition, and rising costs, money laundering continues to pose a significant risk to the global financial system, with criminals seeking to legitimize illicit funds through a series of complex transactions.

According to the half-year report of 2023 released by fintech global, noncompliance to the Anti-Money laundering requirements was the leading source of fines and penalties for financial institutions.

The Financial Intelligence Authority of Uganda published a national risk assessment report in May 2023, which also placed financial institutions as one of the high-threat sectors that can be used to launder money in the country due to their asset size and high cash activity.

This, therefore, requires institutions to enhance their anti-money laundering protocols as a proactive approach to minimizing cases of money laundering, while dealing with customers, to protect their reputation and avoid fines and penalties.

This article explores key strategies which can help institutions in the financial sector to reinforce Anti-money laundering compliance.

i) Know Your Customer (KYC) strategy

A KYC strategy involves procedures and controls which help to ensure that reasonable measures are undertaken to ascertain the identity of the customers, when entering into business relationships or conducting transactions with customers.

An effective KYC strategy is the foundation of any money laundering risk management program. Financial institutions must conduct thorough KYC reviews on their customers, understanding their identity, business activities, and the source of their funds. This involves verifying customer information.

A well-defined KYC strategy also sets out the criteria for categorization of customers based on the perceived level of risk associated with them, which is key in achieving AML compliance.

ii) Enhanced Due Diligence (EDD) strategy

EDD involves a deeper investigation into the customer's background, source of wealth, and obtaining senior management approval before entering some business relationships with customers, where appropriate.

A good KYC program should be reinforced with an EDD strategy for high-risk customers who may include individuals or entities from high-risk jurisdictions, politically exposed persons (PEPs), or clients engaged in complex transactions.

For example, according to Reuters January 2023, Al Rayan Bank was fined 4 million British pounds for their failure to conduct adequate due diligence on high-risk customers.

Regulation 15 (2) of the Anti-Money Laundering Act 2013, requires accountable persons to conduct enhanced due diligence measures in line with the identified risk.

iii) Transaction monitoring

The Reuters news agency on September 13, 2022, revealed that Danske Bank was fined 1.82 million Euros by the Central Bank of Ireland due to their failures in transaction monitoring.

Continuous transaction monitoring is always considered essential in detecting suspicious customer activities. Financial institutions can implement advanced analytics to aid in identifying unusual patterns, such as large cash deposits and unusual fund transfers.

iv) Customer risk profiling

Risk profiling of customer is crucial to ensuring compliance with the Anti Money Laundering Act and regulations. It can be done by assigning risk levels to each customer, whereby

more attention and resources are allocated to high-risk customers, while streamlining processes for the low-risk ones.

The risk profiling strategy of an institution should be updated on a periodical basis to identify new threats, adapt to changing regulations, and adjust their profiling strategies accordingly because money laundering risks evolve over time.

v) Suspicious activity reporting

Financial institutions should also establish clear protocols for reporting suspicious activities to the Financial Intelligence Authority (FIA).

A "suspicious transaction" can be defined as a transaction which is not consistent with the customer's known legitimate business or personal activities or with the normal business of the customer, or a complex and unusual transaction that has no apparent or visible economic purpose.

According to Reuters September 28, 2021, a German online Bank N26 was ordered to pay 4.98 million US dollars for delays in submitting suspicious activity reports. Regulation 39 of the Anti-money Laundering Act 2013 of Uganda requires financial institutions to notify the FIA of any suspicious activity as soon as practicable, in any case not later than 48 hours. Prompt and accurate reporting are, therefore, key requirements to AML compliance in Uganda, and staff should be trained to recognize red flags.

vi) Employee training and awareness

In the current dynamic financial environment, AML compliance should not be a sole responsibility of one department, because criminals are always evolving and getting smarter and more sophisticated in their attempts to hide and disguise illicit money. Achieving a robust anti-money laundering compliance program requires a well-trained workforce to recognize and respond to money laundering risks. Regular awareness campaigns can help keep employees vigilant.

vii) Automating the process

Financial institutions can also leverage technology and data analytics to improve their AML risk management efforts. This can be done by investing in AML software solutions which can analyze vast amounts of data, identify patterns, and generating alerts for suspicious activities.

This will allow the Anti money laundering team to concentrate on analyzing and investigating the results generated from the software, which will reduce the risk of financial crime for the organization.

Conclusion

Having a robust Anti-money laundering assurance program is a critical aspect for financial institutions responsible for fighting financial crime. Such a responsibility requires having a robust AML compliance program which can be achieved by undertaking the above-mentioned initiatives, inter alia.



THE ART OF RESILIENCE

INCIDENT MANAGEMENT MASTERY

HOPE VICTORY SHABA

Information Security Specialist - NSSF



The age-old saying, “It’s not a matter of if, but when, a cyber-attack will happen”, is more relevant than ever before in this fast-evolving domain of technology. Cybersecurity incidents have become an unfortunate reality of our digital lives, casting a shadow of doubt on the security or privacy of data within the various devices and networks that we use. Like a battle fought in the shadows, we find ourselves questioning whether we’ve truly eliminated the lurking adversaries or merely brushed them away momentarily.



Usually, attackers are placed in three main categories, that is: (i) the hackers, (ii) the profit-seekers, and (iii) the sophisticated state-sponsored groups. Understanding the nature of your adversary is pivotal in preparing for the impending storm. While hackers may be out for fun and fame, the financially motivated actors are chasing the almighty dollar. On the other end of the spectrum, the sophisticated groups are after valuable state secrets, even employing spies on the ground to achieve their nefarious goals.

Now, you might be thinking, how can we possibly defend ourselves in this digital world? The answer lies in embracing a multifaceted approach, one that involves understanding the attackers’ tactics, intelligence, and above all, vigilance.

First and foremost, it’s essential to keep a keen eye on DNS (Domain Name System) queries, i.e., the digital footprints

of devices. This is where threat intelligence comes into play. Various companies worldwide classify IP addresses and domain names to discern their malicious intent. If your network is connecting with known malicious domains, as a consequence of malware infections or phishing attacks, it’s time to roll up your sleeves, block the connections and investigate further.

However, vigilance doesn’t stop at monitoring your digital footprint. As a cyber security specialist, communicate with your team and alert them about the impending storm. Picture yourself as the weatherman in the realm of cybersecurity, raising the red flag for your organization. Warn your colleagues about phishing emails and empower them to report anything that appears suspicious to your security team. The power of awareness and a proactive response cannot be overstated.

In the ever-inter-connected world of the internet, your company is just one click away from countless threat actors worldwide. No matter the size of your organization, whether it’s a tech giant or a small business, you must adopt robust cybersecurity measures. The playing field might seem asymmetric, but in the digital realm, your defenses must be just as robust as the biggest names in the industry.

Furthermore, don’t be a lone wolf in this cyber jungle. The power of collaboration cannot be understated. Attend conferences, meetups, talks, and workshops. Share your experiences and learn from others who tread the same path. Cybersecurity is a collective effort, and the more allies you have, the better equipped you’ll be to safeguard your digital kingdom.

Bruce Schneier, a renowned cybersecurity expert, once said, “You can’t defend. You can’t protect. The only thing you can do is detect and respond.” These words hold the key to mastering the art of cybersecurity. Instead of trying to build higher walls to keep intruders out, focus on honing your detection and response capabilities.

Invest in monitoring tools to scrutinize your network inside out. By doing so, you gain a clearer understanding of where the malware has infiltrated, how it's moving, and which systems are compromised. It's like turning on the floodlights in your cyber fortress, illuminating every corner for potential threats.

Additionally, don't underestimate the power of cooperation in the fight against cyber villains. In the event of a cyber incident, coordinate your efforts with vendors and service providers to block the cyber criminal's access and deplete their resources. The more obstacles you throw in their way, the less likely they are to persist; this concept is referred to as the pyramid of pain. Cybersecurity is about making it strenuous for attackers to penetrate your defenses. Although you may never achieve absolute security, you

can certainly make the attackers work harder. Utilize the latest tools, hone your knowledge, and maintain unwavering vigilance. The goal is, therefore, to make the attacker's journey as hard as possible.

Conclusion

The world of cybersecurity is an entanglement of uncertainty, where the only constant is change. By embracing a holistic approach, staying informed, and fostering collaboration, you can navigate these treacherous waters with confidence. While you may never achieve impenetrable security, you can certainly be the vigilant guardian of your digital realm, ready to respond swiftly to any threat that emerges from the dark side of the internet.

HOW DUE DILIGENCE CAN MINIMIZE SUPPLY CHAIN RISKS

ADOLF KAIJA BAGUMA
Operational Risk Manager - NSSF



At the most basic level, supply chain management (SCM) refers to the management of the flow of a product or service, from the procurement of raw materials to the delivery of the product to its final consumer. Supply chain management is a critical component for business continuity and if not managed well, the result can be catastrophic for the operations of any business.



Supply chains are complex networks that involve the production, distribution, and delivery of goods and services. While they are essential for the functioning of businesses, they are also susceptible to various risks. Understanding and mitigating these risks is crucial for maintaining the resilience and efficiency of supply chains. One of the ways of identifying potential SCM risks is by conducting a supply chain due diligence, which is a process by which a company researches and investigates existing and potential suppliers to identify any risks associated with them. Typically, these risks relate to lack of expertise, operational and financial capacity, statutory, governance, ethical, environmental, and societal concerns.

Due diligence (DD) is an important risk preventive mechanism that plays devil's advocate, picturing worst-case scenarios and their potential outcomes on the business if the suppliers were to fail to perform part of the bargain.

Depending on the purpose and context for which due diligence is conducted, it could take different forms, including but not limited to the following:

1. **Business due diligence:** This considers a company's market position, including its growth prospects, supply chain capabilities, governance systems, etc.
2. **Legal due diligence:** This is concerned with ensuring that the company is operating legally and fulfils all its regulatory obligations, such as tax, environmental, social security, and other statutory requirements.
3. **Financial due diligence:** This form of due diligence attempts to examine the company's financial capacity to ensure it can finance its operations in the foreseeable future.
4. **Technical due diligence:** This kind of due diligence is the analysis of a supplier's technical architecture to assess his/her capabilities in terms of both, physical infrastructure, and expertise in fulfilling your needs once they have been engaged.

Conducting effective due diligence is largely a matter of experience and judgment and should be tailored to the extent of the risk. It should, however, be noted that due diligence cannot eliminate all risks inherent in the supply value chain and should not be so expensive to result in a business or project not being cost effective.

Key supply chain risks

i) Ghost/Shell company

An unreliable supply chain is one of the key risks that can undermine the operations of an organization. This may arise from dealing with ghost/shell companies, which have no real operations or assets. These types of companies are often used for illegal purposes such as money laundering, tax evasion, or fraud.

A typical example was in 2014, where the Uganda National Roads Authority contracted EUTAW construction company for a tender of UGX 165Bn and made close to UGX 25Bn as advance payment. It was later established that EUTAW did not exist and had made a misrepresentation that it was a subsidiary of Eutaw Construction Company, Inc, USA. The government lost money in the deal and several officials were arrested and some convicted.

Another case in point is the controversy between NSSF Uganda, Alcon International Limited (Kenya) and Alcon International Limited (Uganda) in the construction of Workers house. All the above cases would have been avoided, had there been a comprehensive DD on the companies before contract award.

ii) Supply chain resilience

Supply chain resilience refers to the ability or capacity of a supply chain to adapt, respond, and recover from disruptions or changes. This capacity is buttressed by the supplier's financial capacity, governance systems, employee competencies, robustness of company technology, etc.

Conducting DD will help to assess the company's ability or capability to adapt, respond and recover from any destructions.

iii) Cybersecurity threats

As supply chains become more digitally connected, they are increasingly becoming more vulnerable to cybersecurity threats.

This interconnectedness can lead to supply chain attacks, whereby a supplier with access to an organization's systems is hacked and the hacker gains access to the organization.

A perfect example of this kind of supply chain attack is the case of SolarWinds whose attack affected many of the other organizations, including the USA's homeland security and Treasury, as well as FireEye, Microsoft, Intel, Cisco, and Deloitte, that were connected to SolarWinds systems.

Before entering any supply contract, it is important to establish whether the prospective supplier or service provider has got a robust cyber security infrastructure that will minimize the impact of cyberattack.

iv) Transportation & logistical challenges

Transportation and logistics are critical components of the supply chain. Risks associated with shipping delays, customs issues, and capacity constraints, can affect the timely movement and delivery of goods and services, leading to increased costs and potential customer dissatisfaction.



A typical example of failure for the contractor to meet their obligation is the Rift Valley Railways (RVR), which in 2006 had been handed a 25-year contract to run the Kenya-Uganda railway. By 2017, their concession was terminated, citing their failure to meet set operating targets, including payment of concession fees.

This risk would have been mitigated had the Ugandan and Kenyan governments conducted a comprehensive due diligence to assess the contractor's technical and logistical capabilities prior to engaging them.

v) Regulatory compliance risks

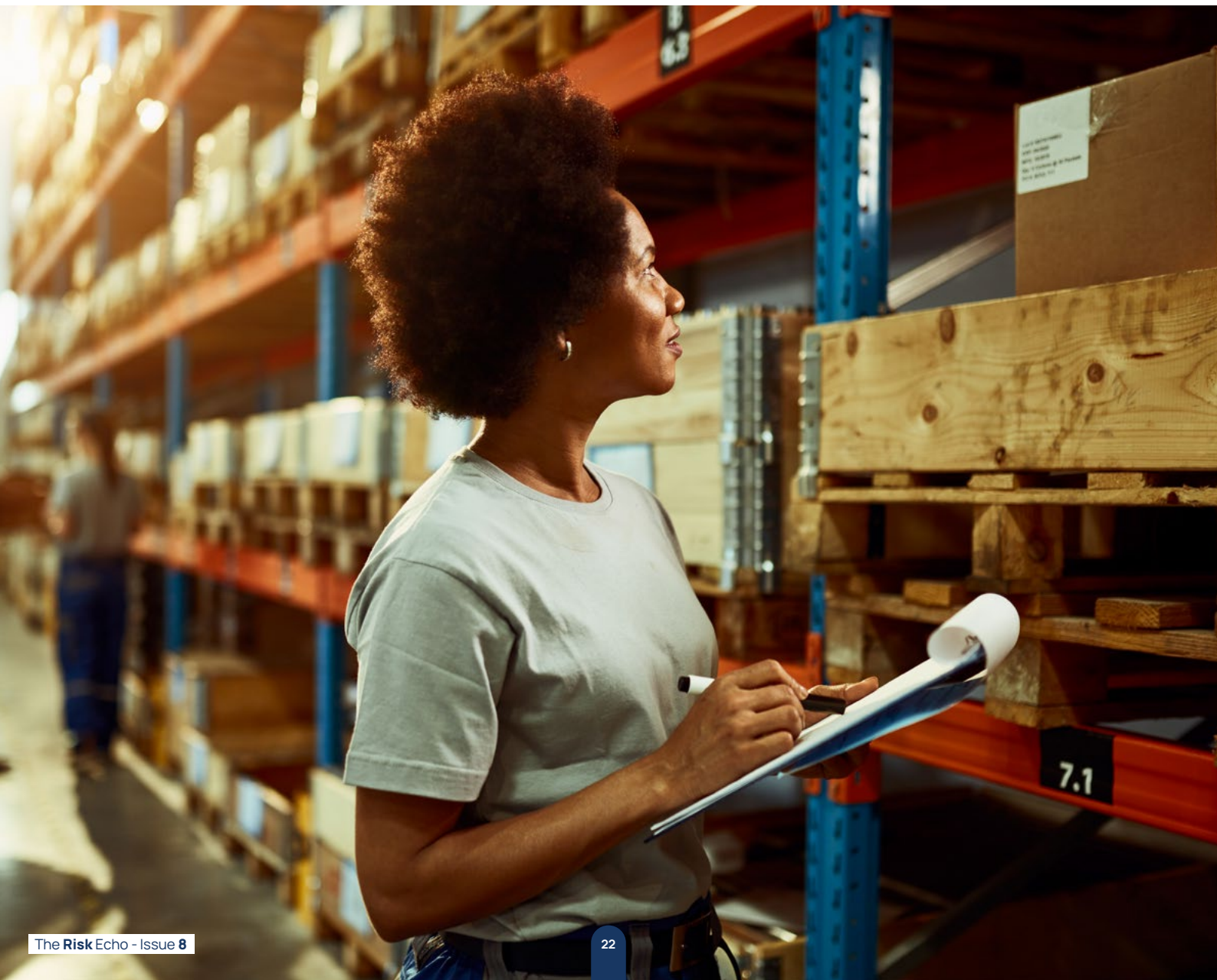
Supply chains are subject to various regulations and compliance standards. For example, government entities in Uganda are required to deal with companies that comply with laws and regulations such as the PPDA Act, Income tax Act, Social Security Act etc. Failure to adhere to these laws can result in consequences ranging from legal sanctions, fines, damage to the reputation of the organization, etc.

Understanding the regulatory compliance status of the suppliers/contractors is critical in minimizing the risks that could arise from their noncompliance; and this can be best done by conducting supplier/contractor due diligence prior to engaging them.

To effectively manage the above-mentioned risks, organizations need to implement robust risk management strategies, including due diligence, contingency plans, diversification of suppliers, technology adoption for better visibility, and ongoing monitoring. Collaboration and communication with supply chain partners are essential for building resilience and responsiveness in the face of unforeseen challenges.

Conclusion

By implementing a supply chain due diligence approach, a company can identify risks that could arise from working with different suppliers. Increasingly, supply chain due diligence is being used to ascertain whether prospective suppliers align with the company's environmental, social, financial, political, governance, legal and other requirements. The bottom-line for due diligence is to reduce exposure to risks associated with the supply chain, whereby critical details about the supplier are known before entering an arrangement to supply or provide the service. Fundamentally, doing due diligence means that you have gathered the necessary facts to make a wise and informed decision.





IS ARTIFICIAL INTELLIGENCE A FOE OR A FRIEND?

JESSE OKUTRE

Operational Risk Specialist - NSSF



AI is an acronym for Artificial Intelligence, which is the theory and development of computer systems able to perform tasks that would normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages (www.coursera.org/articles/what-is-artificial-intelligence)

AI, together with big data, machine learning and Internet of things, is part of the Industry 5.0, also known as the Fifth Industrial Revolution, a new and emerging phase of industrialization that sees humans working alongside advanced technology and A.I.-powered robots to enhance workplace processes.

AI has had a lot of media coverage in the recent times, both positive and negative. You have heard about countries advocating for the regulation for the use of AI, especially after the launch of ChatGPT. The EU, for instance, has drafted a law, the EU AI Act, the first of its kind, to regulate AI. According to an article, "EU AI Act: first regulation on artificial intelligence", on the EU Parliament website, as part of its digital strategy, the EU wants to regulate AI to ensure better conditions for the development and use of this innovative technology. AI can create many benefits, such as better healthcare, safer and cleaner transport, more efficient manufacturing, and cheaper and more sustainable energy. According to BBC, Italy banned the use of ChatGPT, citing privacy concerns. Joe Biden, the American President,

moved fast to sign an executive order to address concerns on AI. All the regulations and authorities coming out strong on the use of AI, show how people are not comfortable with the advancement in the development and use of AI.

However, we have also seen the good side of AI, for example, making headlines in medicine after it shortened the process of medical research that would have taken a long period. The use of IBM Watson health and other AI related technologies are changing the health landscape by helping with diagnosing Alzheimer's disease, cancer, and other difficult-to-detect diseases, at an early stage, which is saving lives.

In Uganda, a murder fugitive was recently nabbed at the Kenyan airport with the help of facial recognition devices. This is one individual who had evaded the authorities for some time after skipping bail.

This leaves one wondering whether AI is a foe or a friend, does it pose a risk to humanity or is it an innovation that makes life easy and good for humanity? These are questions that we will try to debunk in the article.

As a foe: A lot has been shared about the potential of AI; some tech analysts have suggested that in advanced form AI will in future be a threat to humanity (just like in the terminator movies). Below are some disadvantages of AI:



Job displacements

Automation and use of AI technologies is a big threat to employment of humans. Innovators in different sectors are busy automating processes, e.g., in the customer services and support, AI-powered chatbots and virtual assistants have replaced customer services officers. Now it is a common trend, nearly every company has a virtual assistant or chatbot on their website, eagerly waiting to assist a customer. Data processing, loan processors, medical diagnostics, IBM Watson lawyer, etc., are some of these AI-powered automations that are causing job displacements.

Privacy and data security

You have heard about the use of deep fakes both in videos and voice recording. Drake and the Weeknd's hit song, heart on my sleeve, was AI generated and uploaded onto YouTube. Within hours, the video had generated over 1.5 million views; the artist complained, and the video was pulled down. Some thieves had used their voices and identity to generate some views for making money. With growing sophistication in generative AI, more of identity theft and deep fakes cases will be exacerbated, impacting personal privacy.

Bias

There is an Africa proverb that goes as, "until the lion learns to tell its story, the hunter will always emerge victorious". The outcome of information generated by AI or ChatGPT will largely depend on who controls the narrative on the internet, which can potentially have inherent biases. This is likely to generate algorithms bias which can affect decision making. For example, when China launched its own government approved AI ChatGPT, the users tested the application by asking about a possible military takeover of Taiwan, and the response was 99% highly likely.

Human laziness

Excessive reliance on AI and other technologies can lead to diminished critical human skills and decision-making capabilities, and to some extent social isolation, resulting from decreased human interaction. An example in this case is the use of Voice command, using Alex, Siri or Bixby, ChatGPT, etc. It is possible to make purchase orders from home, and everything requested gets delivered. The AI goes ahead to make suggestions for what would be the best options.

There are numerous AI-related technologies that make life easy, but increased use of such technologies is increasingly making humans become lazy and socially distant.

Lack of creativity and emotionlessness

One thing that spooks people about AI is that, at one point these machines may become a danger to humanity, since empathy cannot be replicated in machines. When making sensitive decisions, humans inherently consider the emotional consequences, but AI does not have that ability. It will only make the most optimal decision based on the parameters within which it has been provided, regardless of the impact. This means that machines lack creativity and are emotionless in their decision making.

Obsolescence

Given that AI is developed on pre-loaded facts and experience, to have it function well, it would continuously require improvement. Usually, AI is developed to help ease repetitive tasks and routines, however, if there is a slight improvement or change, there will be need to manually code and improve the performance of AI. These continuous improvements can be costly, hindering regular upgrade of the machines, thus making the lifespan of the AI short.

However, instead of viewing AI as a threat to, say job replacements or human life, AI technologies should be viewed as tools for augmentation. AI can complement human capacities such as handling routine and repetitive tasks and take on extremely risky tasks.



Despite those challenges, AI can be considered "A FRIEND"; like the saying goes, "Every cloud has a silver lining". Below are some of benefits associated with AI:

Constant availability

Ever since internet made the world a global village, it has been imperative for businesses to keep their front offices always open to customers 24/7, which means that customers are served at any time of the day.

This is a task that humans could not accomplish with ease, however, with AI this has been made easy using chatbots and virtual assistants. These chatbots are fast in-service delivery and more reliable when giving feedback to customers.



Reduced or zero risks

Developers have built AI robots and machines to minimize the exposure of human beings to risks in manufacturing, exploration, wars and medical fields, etc. AI has reduced the exposure to risk in several ways; for example, during the Covid-19 pandemic, to reduce chances of infection for medical personnel, a researcher developed robots that could help in taking care of the sick by e.g., delivering medicine, foods, and other items, to those that were isolated. This reduced the risk of exposure to the virus by medical personnel.

Increased efficiency

The use of AI significantly improves efficiency and reduces human error in execution of various tasks. Let us take an example of the current wars in Europe- Russia against Ukraine and Israel against Palestine; all the countries are using AI-powered drones that have greater precision and limited casualties on the attacking side.

These drones are AI-auto piloted and can identify enemy targets and destroy them without human assistance. We have seen the NASA's ingenuity helicopter working on mars and delivering results to the earth without human intervention, which has improved the scientist knowledge about the neighboring planet.

Improved products development and service delivery

Use of AI in product development and service delivery has greatly improved customer experience. For instance, online delivery companies have greatly leveraged on data analytics and AI to deliver customized product to their clients.

Faster decision-making

AI can be used in organizations to make faster and more informed decisions. This is particularly valuable in high-stake environments, where decisions must be made quickly and accurately to prevent costly errors or to save lives. In developed economies, AI-powered analytics is used by organizations and individuals to make informed decisions in purchasing, investment, travel, disease diagnosis, etc.

Ease of work

Generally, AI makes life easier; things that seem hard to accomplish manually can be made easy with the use of AI. AI enhances and complements human skills and competences. Let's take an example of AI in the medical fields; the IBM medical assistant, which is an AI-powered tool, has helped doctors and medical researchers analyze patients' data, identify potential health risks, and develop personalized

treatment plans for patients. This has led to better medical treatment for patients and accelerated the development of new medical solutions and technologies.

It seems the development of AI and associated technologies is unstoppable; one only needs to harness the benefits of AI while mitigating the associated risks.

How to mitigate the downside of AI:

i) Regulation

Developers of AI technologies are known to use vast sets of personal data without the knowledge of the owners; this can lead to privacy violations and misuse of sensitive information.

Therefore, enacting regulations and establishing ethical standards for regulating the development of AI can ensure ethical use of AI, thus reducing on incidences of privacy violations.

ii) Collaboration between humans and AI

Advancements in AI are making work and life easy; therefore, this calls for education and training to encourage collaborative partnership between AI and humans. AI in good hands fosters creativity and innovations, which is a recipe for increased productivity.

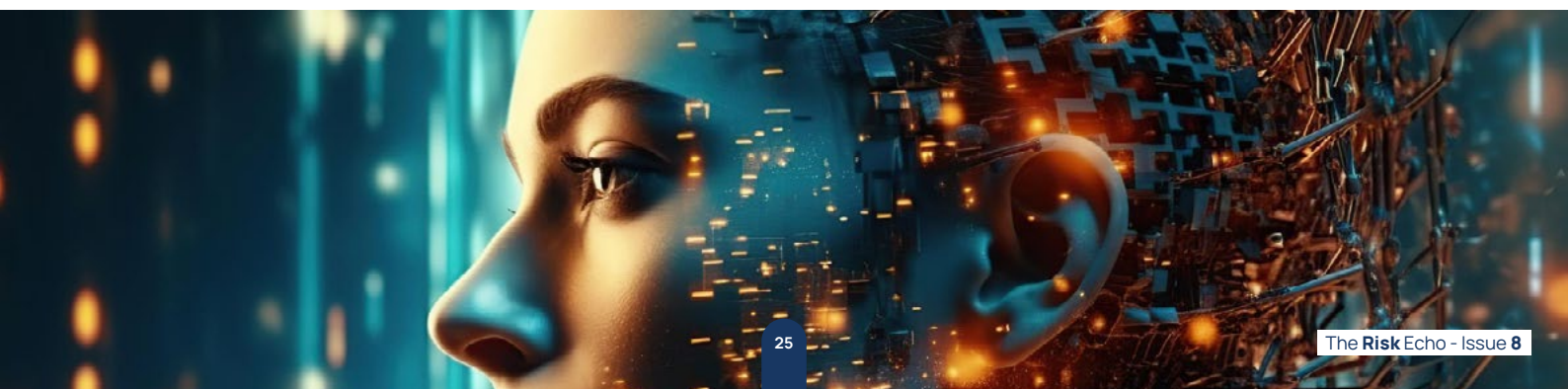
iii) Humans in control

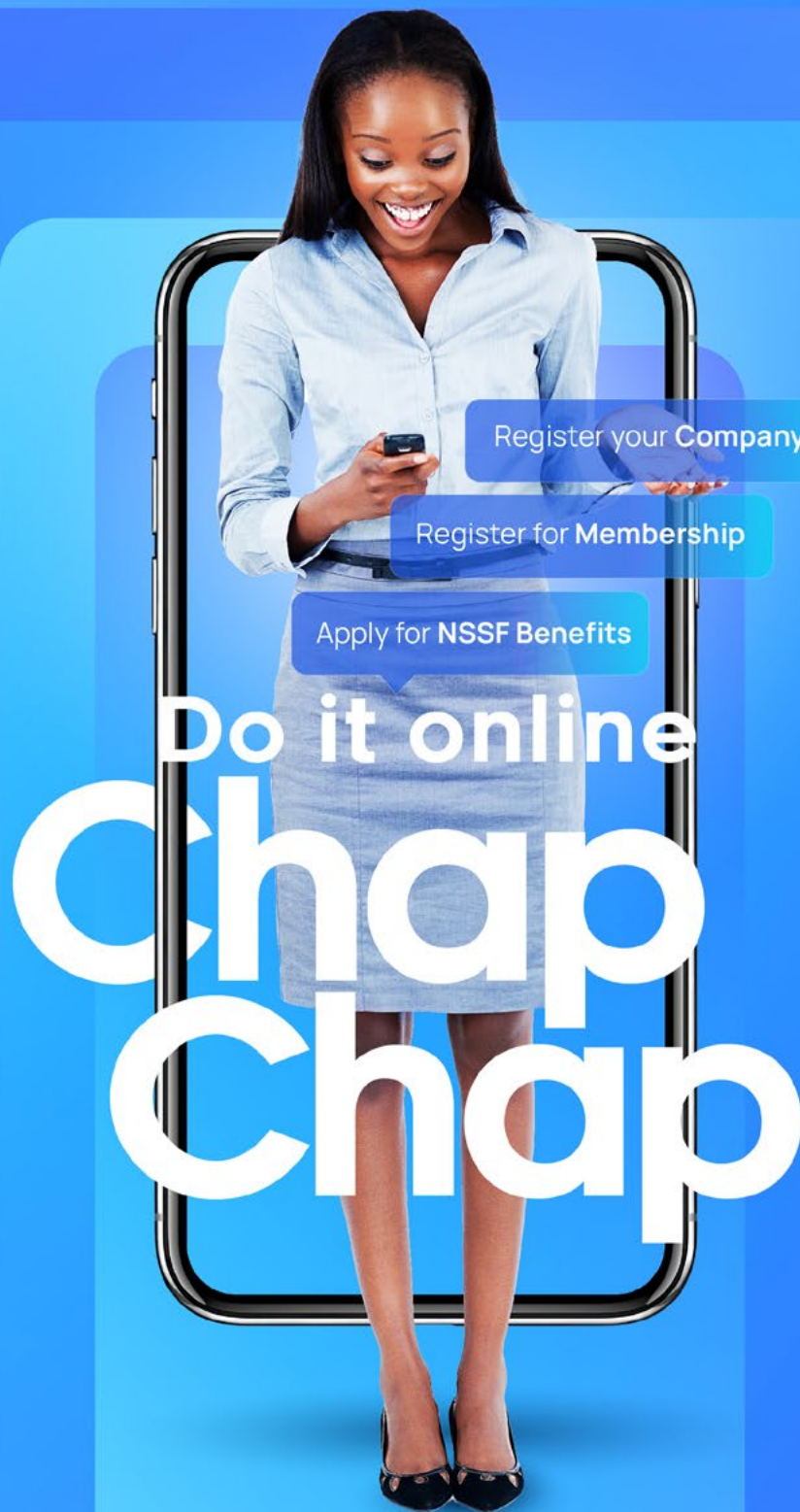
Even as these AI technologies help in execution of tasks; human beings should remain in control when it comes to critical decision-making processes. While AI can provide valuable insights and recommendations, humans should have the final say, particularly in areas that involve ethical considerations, complex judgment, and the well-being of individuals.

Conclusion

There are mixed sentiments about the development and advancement in artificial intelligence; those that are worried about the advancement of AI, despite acknowledging the enormous benefits of AI in all spheres of life, they cite ethical and moral considerations as explained above. That notwithstanding, the advancement of AI seems to be unstoppable because of its potential to completely transform society for the good of mankind.

To minimize the negative repercussions of AI, it is imperative that specific regulations for AI are put in place to ensure that the development and use of AI does not undermine the very existence of mankind- other countries need to borrow a leaf from the EU.





Skip the hassle. Conveniently register, apply for NSSF Benefits and do much more anytime anywhere on the **NSSFGo App, Web** or ***254#**

Visit www.nssfgo.app or download the **NSSFGo App** today.



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

*Terms and Conditions Apply.





Having trouble with
the **NSSFGo** App?



Delete and install the
enhanced version

Replace your old app with the new and improved
NSSFGo App for a seamless experience.

Visit www.nssfgo.app or download the new **NSSFGo App** from



Enter the **Phone number** or **Email address** used to register with NSSF.

Enter the **One-time password** sent to your phone number or email address and you are good to go.

Don't worry if you can't recall the Phone number and Email address
you gave us. Contact us to update your details.

Call 0800 286 773 toll-free

customerservice@nssfug.org

+256 784 259 713

Visit the nearest branch



PROTECTING THE SCADA NETWORK

BRIAN NUWAGABA LUDOVIC

Ag. Information Security Manager - NSSF



SCADA, which stands for Supervisory Control And Data Acquisition, is a system of software and hardware components that enable industrial organizations to control industrial processes, both remotely and locally, monitor and gather real time process related data, directly interact with elements like sensors, pumps, motors, etc. and record events happening on these elements.

SCADA systems are everywhere. Virtually, wherever one may look, there will be a SCADA system running in the background. Take the example of your everyday tap water whose safety we have all grown accustomed to taking for granted. There is a SCADA system behind the wastewater management process that ensures your tap water is safe. Consider everyday commodities like alcohol, soft drinks, sugar, soap, medicine, etc. whose processing relies heavily on these SCADA systems. SCADA systems are essentially the backbone of many modern industries spanning sectors such as oil and gas, transportation, water and waste management, manufacturing, to mention a few.

Ok, so what is the risk?

Imagine, an adversary was able to penetrate a nation's wastewater management systems. This adversary would be able to alter the behavior of the hardware components responsible for measuring the right amounts of disinfectants used to clean water, thus making the water potentially poisonous for millions of consumers. Take another example of a potential attack on the SCADA systems that manage a nation's power generation facilities. Such an attack could lead to a nationwide power blackout. Entities such as hospitals running life support equipment would certainly be impacted heavily, with possible loss of life. To make matters worse, majority of these industrial components were originally built with no basic security in mind at the time, as hackers were not much of a threat.

Whereas attacks on your typical corporate networks can be devastating, seldom are they life threatening. Sure, such an attack on a corporate network can lead to frustrated customers who can't access a particular service, nonetheless, they will still be alive.

On the flip side, an attack on SCADA based systems can be life threatening as seen from the examples above. This is a clear example of how cyber security risk has evolved to impacting physical infrastructure, and thus everyday life as we know it in the literal sense. This begs the question,

How do we protect these systems?

There are several measures that can be taken to safeguard such systems or at the very least, significantly minimize the impact thereof. At the heart of this, these measures can largely be categorized into 3 information security pillars, which are people, processes, and technology.

i) People

Kaspersky, a well-respected information security vendor, in its Spam & Phishing report, indicated that the number of phishing attacks doubled in 2022 to over 500 million. Cybercriminals are increasingly turning to phishing as a way to compromise networks through tricking users into unintentionally doing malicious activities.

Generally, people are usually the weakest link in the entire chain. Carrying out organization wide information security awareness activities can significantly reduce this risk, as staff become more knowledgeable in identifying phishing methods.

For effective dissemination of information about phishing activities, it is important that the organization uses a multi-faceted approach, as people respond differently to different media of communication. In an article titled, Measuring and Evaluating the Effectiveness of Security Awareness Improvement Methods, by Eszter Diana Oroszi, it was found that organizations that relied on a mix of various methods of delivering such awareness activities benefited the most by having staff more engaged and learning more compared to those that did not make use of multiple strategies to deliver the same activity.

ii) Processes

Processes, which are the second pillar of cybersecurity, form the framework for governance and provide procedures that need to be followed. As an example, a manufacturing plant may require that before changes are deployed in production, appropriate approval should be obtained, and there should be proper segregation of duties (Maker-Checker principle).

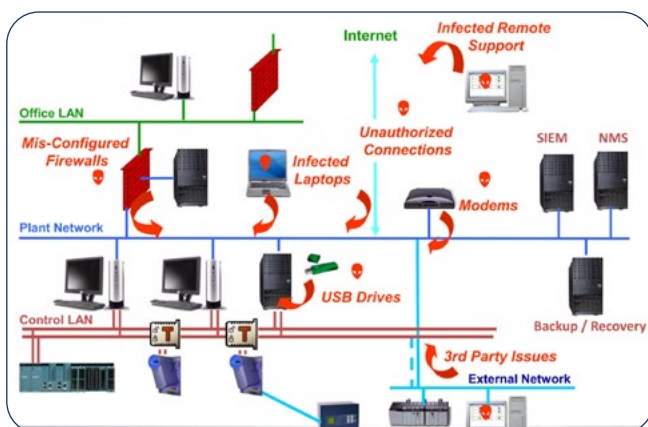
Organizations can opt to adopt and get certified based on internationally recognized information security standards like ISO 27001:2022. Such certifications provide confidence to your end consumers that you have taken measures to ensure the security of your production systems and data. Attaining this certification does not mean that you will not get hacked, but it certainly instills a higher level of trust from your customers, knowing that another external party did audit your organization.

The importance of procedures such as change management, vulnerability management, to mention a few, become even more pronounced with SCADA systems given the level of impact these networks have on our lives.

iii) Technology

In the space of technology, there are several measures that can be taken, including but not limited to:

a) Network isolation



Source: Building a Cyber Security Operations Center for SCADA/ICS Environments by Shah Sheikh

Isolate the SCADA network from the corporate network. Isolation of networks comes with benefits such as a reduction in blast radius in the event of a compromise of either network. This isolation creates both logical

and physical barriers between the two networks. Often technologies such as firewalls are used to provide traffic filtering/inspection and to control access. The image above illustrates some of the attack points malicious actors can use to access the plant floor.

b) Patch management

Patching is aimed at plugging holes in a vulnerable system so that hackers cannot abuse them. Key to note here is that, unlike the corporate networks where patch management is often rapid, reactive, and continuous on a regular basis, this is not feasible with SCADA systems. More comprehensive testing and support from the SCADA vendors is required, resulting into a much slower patch cycle, compared to corporate networks.

There are, however, compensating controls that the internal security teams can adopt during the slow patching cycle. An example of such could be to reconfigure the product, by disabling services like HTTP (Hyper Text Transfer Protocol), used for communication over the internet. A product reconfiguration like this can help provide an added layer of security, whilst the patch management cycle is still running its course.

c) Enhance monitoring and detection

Similar to what is done for the corporate networks, monitoring is required to be able to detect and stop cyber-attacks from progressing and eventually resulting into data loss and/or physical damage.

However, it should be noted that the tools used for monitoring and detection should be "SCADA-technology aware". For example, a typical standard corporate network firewall and intrusion detection system will likely not understand SCADA specific protocols.

d) Incident response playbooks

Playbooks are documented standard procedures and steps to be taken whilst responding to an incident. Having these documented and rehearsed over time, helps to identify any weaknesses associated with them and proactively address them (weaknesses). It also helps to build confidence in the incident response teams, enabling them to better deal with an actual incident when it happens.

Conclusion

A hack on a SCADA system can literally become a life-threatening situation. Whereas the list of measures above is by no means exhaustive, organizations can significantly reduce the technical, financial, and reputational impact that the hack could have if such measures are in place.

THE NEED FOR ALTERNATIVE INVESTMENTS: NAVIGATING THE PATH TO FINANCIAL SUCCESS

ROBERT MASIGA

Investment Risk Specialist - NSSF



Investing is a critical component of wealth management, and the choice of assets is pivotal in achieving financial goals. In the world of finance, investors are presented with a wide array of options, including traditional assets and alternative investments. Each category has its unique characteristics, risks, and rewards.

This article aims to make a case for alternative investments to ensure effective portfolio diversification, shedding light on factors that investors should consider when building a diversified portfolio.

To begin with, traditional assets, also known as conventional assets, are the bedrock of investment portfolios and include equities, fixed-income securities, and cash. The arguments for traditional assets include but not limited to:

a) Stability and consistency of returns

Traditional portfolios, with investments in traditional assets like bonds and equities, have historically provided a steady source of income and long-term capital appreciation. The stability and consistency of returns provided by traditional assets are paramount for wealth creation, which is the main objective of investment.

b) Liquidity

Traditional investments are often highly liquid, allowing investors to buy and sell assets quickly, with minimal transaction costs. This liquidity provides flexibility in portfolio management.

c) Transparency

Traditional investments are generally transparent, with publicly available pricing and performance data, making it easier for investors, even the less educated, to assess their holdings.

d) Ease of management

Traditional assets can generally be handled by even the less experienced in the field of investment.

Nevertheless, traditional assets have various disadvantages, including but not limited to:

a) Market risk

Traditional assets are subject to market risk, such as changes in equity prices, interest rate moves or foreign exchange fluctuations, meaning that their value can fluctuate based on economic conditions, investor sentiment, and external events.

b) Inflation risk

Traditional assets, especially cash and bonds, may not keep pace with inflation, leading to a loss of purchasing power over time. This loss in value is because of the valuation principle of discounting, that is, inflation is inversely related to the value of a bond.

c) Low yield in low-interest environment

In periods of low interest rates, bonds and cash may offer relatively low yields, limiting wealth creation. When yields are low, the periodical payments to the holders of these assets are usually low, with a potential to limit attainment of an individual's objectives.

d) Credit and default risk

Bond investments, particularly high yield bonds (corporate bonds), carry credit risk, arising from a possibility of bond issuers defaulting on payments, resulting in potential losses for bondholders.

On the other hand, alternative investments encompass a wide range of non-traditional assets, including private equity such as venture capital, hedge funds, real estate, derivatives, farmland, commodities, etc. These assets can provide diversification beyond the confines of traditional asset classes. However, a number of considerations have to be taken into account before resources are deployed in these kinds of assets.

The following factors favor the need for alternative investments in one's portfolio of traditional assets:

i) Diversification

Alternative investments encompass a wider array of assets, which have low correlations with traditional assets, providing better diversification and reducing portfolio volatility. The low correlation implies that if traditional assets are doing badly during a particular period, alternative investments can perform well in the same period. In general, a lower correlation mitigates the risk of volatility in the portfolio.

ii) Potential for higher returns

Some alternatives, such as private equity or venture capital, have the potential for higher returns than traditional assets, although they come with a higher risk. The higher return conforms to the adage that the "higher the risk, the higher the return".

iii) Hedging against volatility

Alternatives like gold or real estate can act as hedges against inflation and market volatility, protecting the portfolio value during economic downturns. A hedge in this case means a way of protecting oneself against financial loss or other adverse circumstances.

iv) Portfolio customization

Alternative investments provide investors with the ability to tailor their portfolios to specific risk-return objectives. This customization can help align the portfolio with the investor's unique preferences, goals, and risk tolerance.

v) Innovation and growth

Investing in alternative assets, especially in areas like venture capital and private equity, provides exposure to innovative and rapidly growing companies. This exposure to potential high-growth opportunities can contribute to overall portfolio performance.

vi) Unique opportunities

Alternative investments offer access to unique opportunities not available through traditional markets, such as investing in private equity like startups, commodities like farmland, real estate such as apartments and rentals.

Nonetheless, alternative investments also have various disadvantages that should be considered before a decision is made. Among the challenges associated with alternative investments, include the following:

a) Lack of liquidity

Many alternative investments are not liquid, making it challenging to buy or sell them quickly without significant costs and/or delays. To access the invested funds, set requirements such as lock-in periods have to be met, which in some instances may be years.

b) Complexity

Alternatives often involve complex strategies, structures, and regulations, requiring a higher level of expertise and due diligence for inclusion in a portfolio mix, for which a lay investor may not be able to navigate.

c) Volatility of returns

Alternative investments can be riskier than traditional assets due to factors like limited information, illiquidity, restrictions on transfer, lack of a secondary trading market, etc.

d) Limited regulation

Some alternatives, such as private placements, are subject to limited or no regulatory oversight, increasing the risk of fraud or market manipulation.

e) Difficulty in valuation

Valuing alternative investments can be challenging due to lack of standardized pricing mechanisms for illiquid assets.

It is important to note that both, traditional assets and alternative investments have advantages and disadvantages, and each's suitability depends on an investor's goals, risk tolerance, and time horizon. Traditional assets offer liquidity, transparency, and a long history of performance, while alternative investments provide diversification, the potential for higher returns, and low correlation with traditional assets. However, they often come with greater complexity, longer investment horizons, and lower liquidity.

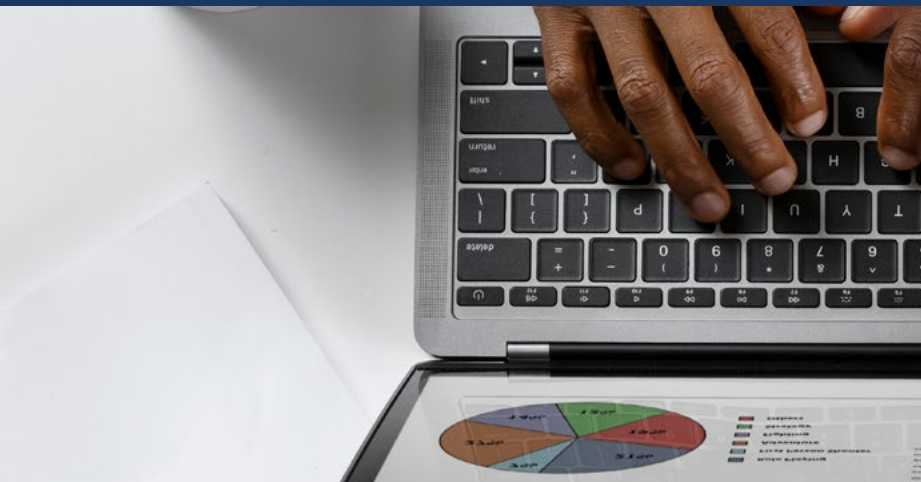
Conclusion

It is important to note that a well-diversified portfolio often includes a mix of both traditional assets and alternative investments to balance risk and return. Investors should carefully consider their financial objectives and risk appetite when deciding on the optimal allocation between these two categories. Ultimately, the key to successful investing lies in building a portfolio that aligns with an individual's goals, while effectively managing risk in an ever-evolving financial landscape.

EMPOWERING SMALL BUSINESSES: THE IMPERATIVE OF COMPUTERIZED ACCOUNTING SYSTEMS IN MANAGING RISK

CHARLES KATENZA

Audit and Compliance manager,
Multi-Community Based Development Initiative



In the dynamic landscape of modern business environment, small and medium enterprises (SMEs) face numerous challenges, with financial management standing out as a major challenge for them. Many of them still use the manual system of recording transactions and reporting financial information.

Computerized accounting is defined by Alan & Frank Wood (2005) as a “total suit of computers that together comprises all inputs, storage, transactions, processing, collecting and reporting of financial transaction data”.

In this article, I explore why the adoption of computerized accounting systems is not only advantageous in ensuring accurate accounting records, but also essential for mitigating risks and fostering sustainable business growth. I also investigate the drawbacks of computerized accounting systems, providing valuable insights for risk management in the financial landscape.

To begin with, the following are the benefits of computerized accounting system:

Accuracy and error reduction: The foundation of financial integrity

In manual accounting, the risk of human error looms large. Incorrect data entry, miscalculations, and discrepancies can have cascading effects on financial statements.

Computerized accounting systems automate calculations, minimizing the likelihood of errors and ensuring financial accuracy that forms the bedrock of sound decision-making.

Efficiency: Unlocking productivity and strategic focus

Manual accounting can be time-consuming and yet time is a precious commodity for businesses, SMEs inclusive. Computerized systems streamline repetitive tasks, such as data entry and reconciliation, freeing up valuable time for business owners to focus on strategic initiatives and growth opportunities.

Cost savings: Benefit beyond the bottom line

While there is an initial investment in software and training, the long-term cost-savings are substantial. Automated processes reduce the need for excessive paperwork, lower the risk of costly errors, and minimize the labor required for manual accounting tasks, contributing to more efficient and cost-effective operations, which can greatly improve on the business brand.

Improved financial management: Navigating complexity with confidence

Small businesses often grapple with complex financial management requirements. Computerized accounting systems provide real-time access to financial data,

empowering SMEs to make informed decisions, manage cash flow effectively, and plan for the future, with a level of financial insight that manual systems struggle to match.

Compliance and reporting: Navigating regulatory seas safely

In an environment where regulatory requirements are ever-evolving, adherence to regulatory requirements is non-negotiable. Computerized systems facilitate compliance with tax regulations, accounting standards, and other statutory obligations. Automated reporting features further simplify the preparation of financial statements, ensuring SMEs navigate regulatory seas safely.

Scalability: “Growing without growth pains”

As SMEs expand, their accounting needs become more complex. Computerized systems can seamlessly scale to accommodate increased data and transaction volumes, providing a flexible solution that grows with the business without introducing operational constraints.

Integration with other systems: Building a cohesive business ecosystem.

In the interconnected world of business operations, integration is key. Computerized accounting systems can integrate with other business systems, such as inventory management or customer relationship management (CRM), creating a cohesive ecosystem that enhances overall efficiency and decision-making.

Ease of auditing: Transparency and accountability at the forefront

Audits are an integral part of financial governance. Computerized systems facilitate auditing processes with digital records, audit trails, and the ability to generate comprehensive reports swiftly. This transparency does not only satisfy regulatory requirements, but it also instills confidence in stakeholders.

Customer and vendor relations: Fostering trust through efficiency

Efficient invoicing, timely payments, and accurate financial transactions contribute to positive relationships with customers and vendors. Computerized accounting systems enable SMEs to manage these interactions with precision, fostering trust and reliability in business relationships.

The adoption of computerized accounting systems has become universal, promising efficiency, accuracy, and streamlined financial processes.

However, while these systems offer numerous advantages, it is essential to shed light on the potential pitfalls that are associated with them.

Initial implementation costs

One of the primary drawbacks of computerized accounting systems is the significant upfront investment required for software licensing, hardware upgrades, and employee training. Small and medium-sized enterprises (SMEs) may not have the necessary resources for the initial

implementation of computerized accounting systems, which is one of their major barriers against automation of accounting processes.

Technical issues and downtime

As with any technological system, computerized accounting is susceptible to technical glitches, software bugs, and hardware failures. These issues can lead to downtime, disrupting daily operations and potentially causing financial inaccuracies. Additionally, resolving technical problems may require specialized expertise, adding an extra layer of complexity.

Security concerns

The digitization of financial data introduces a new realm of security challenges. Computerized accounting systems are vulnerable to cyber threats, including data breaches, hacking, and malware attacks. Protecting sensitive financial information becomes paramount, requiring robust cybersecurity measures and constant vigilance to mitigate potential risks, which may be too expensive for SME.

Dependency on skilled personnel

The effective use of computerized accounting systems relies heavily on skilled personnel. Companies may face challenges in finding and retaining qualified professionals who can navigate the intricacies of the software.

Lack of customization

Many off-the-shelf accounting software solutions may lack the flexibility needed to accommodate the unique requirements of certain industries or specific business processes. This limitation can hinder organizations from tailoring the system to meet their evolving needs, forcing them to adapt their processes to fit the constraints of the software.

Obsolete technology

The rapid pace of technological advancements can render a once cutting-edge accounting system obsolete. Organizations may find themselves grappling with the need for frequent updates or even complete overhauls to keep pace with evolving industry standards and regulatory requirements, leading to additional costs and disruptions.

While computerized accounting systems have undoubtedly revolutionized financial management, it is crucial to recognize the potential drawbacks inherent in their adoption. By proactively addressing these limitations, organizations can develop risk mitigation strategies, ensuring a more resilient and secure financial landscape.

By and large, the adoption of computerized accounting systems is not merely a technological choice for SMEs, it is a strategic imperative for managing risks, ensuring financial integrity, and fostering sustainable growth. As the business landscape continues to evolve and regulatory compliance continues to be tightened, SMEs equipped with these advanced tools will not only navigate risks more effectively but also position themselves for success in the ever-changing world of commerce.

PROTRACTED REFUGEE SITUATION: CAUSES, CHALLENGES & SOLUTIONS

MR. SAMUEL OPONO

Research Assistant, Faculty of Interdisciplinary Studies, Mbarara University of Science and Technology.



The 1951 Refugee Convention and its 1967 Protocol provides the primary and universal definition of who a refugee is; which is contained in Article 1(A) (2) of the 1951 Convention, as amended by its 1967 Protocol, defining a refugee as someone who: "Owing to well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or who, not having a nationality and being outside the country of his former habitual residence, is unable or, owing to such fear, is unwilling to return to it".

According to the UNHCR global trends, by the end of 2022, over 108 million people were forcibly displaced worldwide. Seventy-six percent (76%) of these world refugees and other people who require international protection by the end of 2022, were hosted in low- and middle-income countries. During the same period, the least developed countries provided asylum to 20% of total global refugees. The neighboring countries to the countries generating refugees hosted 70% of refugees and other people in need of international protection.

Uganda, the highest refugee hosting country in Africa and among the top refugee hosting countries in the world, hosts over 1.5 million refugees, majorly from the neighboring countries and the wider region, including South Sudan, Democratic Republic of Congo, Burundi, Somalia, Rwanda, Kenya, Ethiopia, and Eritrea among others.

Some refugees have been living in the host countries for so many years, and the UNHCR refers to such a situation as a protracted refugee situation. UNHCR explains Protracted Refugee Situations (PRS) as those in which at least 25,000 refugees from the same refugee producing country have



been living in exile for over five consecutive years. Refugees trapped in these situations usually find themselves in a state of limbo: it is neither safe for them to return home, nor have they been granted permanent residence to stay in another country - either the first asylum country or the third country.

By the end of 2022, about 23.3 million refugees and other people who require international protection were living in protracted situations, an increase of more than 7.1 million refugees, compared with the numbers in the previous year. According to the UNHCR global trends, by the end of 2022, there were 57 protracted situations in 37 different host countries. These protracted refugees are in a state of limbo and are uncertain of their future: whether they will be repatriated, locally integrated, or resettled in the third country.

Refugees trapped in protracted situations often face significant protection challenges and restrictions on their rights. They may be deprived of freedom of movement, legal employment, access to land and systems of justice. Children may also have limited or no access to education.

The lack of economic opportunities forces displaced families into dangerous coping mechanisms. Women and children are especially vulnerable to child and early marriage, child labor and sex trafficking.

Drivers of the Refugee Problem



Displacements are driven by persecution, conflict, violence, human rights violations, climate change, famine, and other events profoundly disturbing public order.

Protracted refugee situations are engendered and perpetuated by incessant conflicts and futile peace processes in the countries of origin. For example, conflict persisted under former President Nkurunziza of Burundi, when it was clear that he was bent on clinging to power. Conflict endured while the peace process was ongoing, being brokered by Ugandan President Yoweri Kaguta Museveni and the former President of Tanzania Benjamin Mpaka. In South Sudan, in the face of peace process mediated by Inter-Governmental Authority on Development (IGAD), conflict continued between government forces and forces loyal to the former Vice President Riek Machar. The 2015 peace agreement and cessation of hostilities were constantly violated. In DRC, conflict continued in the presence of the largest United Nations peace keeping operations in the world, compounded by the unwillingness of the then President Joseph Kabila to organize elections. All these continued to increase the inflow of refugees to the neighboring countries.

Protracted refugee situations are artificially created and are avoidable effects of involuntary population flows; they are the consequences of political actions in the country of origin.

Negative effects of PRS

The presence of PRS can breed several political and security concerns for host countries, the countries of origin, regional actors, and the international community.

The persistent presence of large refugee populations has been associated with international and regional conflicts, by fueling instability in the neighboring countries, prompting intervention, and occasionally encouraging armed elements within camps to organize into an insurgency, resistance, and terrorist groups. Like in some areas of the African Great Lakes region,

the Horn of Africa, West Africa and Southern Africa, the Middle East, South and Southeast Asia, and Central and South America.

Security issues such as arms trafficking, drug smuggling, the trafficking of women and children, and enrollment of child soldiers and mercenaries, can and take place in some of the camps and urban areas accommodating displaced populations.

Apart from generating direct security situations, prolonged refugee situations can bring about indirect conflicts with host communities. Tensions between refugees and host community members often spring up from the perception that refugees receive special treatment, particularly with regards to accessibility of social services like health and education which may be hard to access by rural host populace, yet the services may be freely available in the refugee camps for refugees.

In a similar vein, decreasing humanitarian assistance may prompt some refugees to resort to illegal coping strategies like banditry, prostitution, and petty theft, which increases local security concerns.

In Sub-Saharan Africa, large forcible movements of people in view of their effects on the national security concerns, most of the time end into host government's decision to close borders to people on the move, refusal to grant asylum, incarceration of refugees and refoulement. Refugees are used as national scapegoats, culminating to xenophobic and acrimonious attitude towards refugees.

Additionally, lack of clear response strategies to refugee situations in Sub-Saharan Africa increases frustration of both citizens and governments regarding protracted refugee situations in their countries; and the UNHCR acknowledges that the global refugee protection system may gradually fragment and weaken. Moreover, several governments also use national security concern and public interest to rationalize their coercive refugee policies.

Practical interventions to PRS problem

Refugees are a sign of global stormy times and PRS have been acknowledged as a burning international issue that requires urgent consideration as well as long-range strategies. PRS demand durable solutions to enable refugee to rebuild their lives with dignity. Three possible durable solutions: voluntary repatriation, local integration and resettlement to a third country. These are internationally recognized UN solutions.

- **Voluntary repatriation** - to their country of origin is considered the best solution, but it is only possible if conditions that have forced them into refuge have ended, so refugees can safely return to their home countries. Repatriation cannot be forced on refugees and must be supported by both countries of origin and asylum.
- **Local integration** - is an alternative for those who can't return home. It allows refugees to remain and become citizens of their country of asylum. Refugees are granted citizenship by naturalization in the host country - first country of refuge- but host countries seldom do this.

- **Resettlement** - allows refugees to move to a third country that has accepted to grant them permanent residence. The most vulnerable refugees are given priorities for resettlement, and due to stringent selection process, less than 1% of refugees succeed in being resettled to a third country.
- Additionally, other interventions such as the ones below can help alleviate the situation:
- **International solidarity:** Governments from developed and developing countries in conjunction with multilateral organizations, have pledged to support one another in tackling refugee problems. For example, at the 2016 Leaders' Summit on Refugees and Migrants, Uganda stood out on its progressive refugee policies, which grant refugees right to work, right to go to school and right to access land. No wonder, Uganda falls among the first countries to have access to funding through a new channel of the World Bank's 18th replenishment of its International Development Association (IDA18), established to make available more concessional financing to low-income countries hosting large numbers of refugees.
 - **Burden sharing:** Researchers recognize that a cooperative and collaborative approach and practical principles based on burden sharing between countries of origin, host countries and resettlement/third countries, can lead to successful outcomes.
 - **Humanitarian organizations:** Humanitarian organizations have played a big role in providing reliefs to refugees, once they arrive in the country of asylum. A collaborative approach involving a wide range of UN agencies, NGOs and other actors have helped in dealing with PRS.
 - **Mainstreaming host communities in humanitarian assistance:** Programmes that include both refugees and host communities as beneficiaries of development interventions, including resource sharing, are gaining prominence as part of the solutions to ameliorate refugee-hosts conflicts. Humanitarian actors do not only focus on refugees but also direct reasonable support to host communities, host members will most probably relate well with refugees.
 - **Land acquisition:** As part of the attempts to find solutions to refugee-host conflicts and promote integration of refugees in host communities, is to first of all, respond to the question of land acquisition for settling refugees. This could lead to acceptable terms of engagement by hosts or outright disagreement over the land. Where bargain over land for camp/settlement constructions is devoid of disagreements, positive host-refugee relations ensue.

Conclusively, refugee flow and PRS are evidently a global challenge that requires solidarity between countries in the global south and their counterparts in the global north, to implement both the temporary and long-term legally recognized durable solutions to tackle the refugee challenge and the underlying causes that push communities to flee their home countries.



Source: <https://africasacountry.com/2021/04/essentialism-and-the-making-of-african-refugees>
Image credit: Julien Harneis via Wikimedia Commons CC BY-SA 1.0.

A woman with dark curly hair, wearing a straw hat and a blue and white plaid shirt, is smiling and leaning against a large, white, metal milk can. The milk can is sitting on a green-painted wooden post. The background is a barn with wooden beams and other milk cans.

**NSSF
FINANCIAL
LITERACY
PROGRAM**

Become better

Sign up for the free **NSSF Financial Literacy Program** and start your journey to financial freedom.

To apply, visit www.nssfug.org/financialliteracy or dial *254# or Call 0800 286 773 toll-free for details.



THE GOOD, THE BAD AND THE UGLY OF HIRING HIGHLY TALENTED PEOPLE

BRIAN B. MUKALAZI

Finance & Strategy Expert
Chief Executive Officer,
Talis Consults Ltd



In February 1974, after eighteen months of dropping out of college, Steve Jobs decided to look for a job. One day, as he searched the papers, he came across a job advert that caught his eye. It was a technician job opportunity at a video game manufacturing company named Atari. His Biographer, Walter Isaacson, wrote that, on that same day, Steve Jobs, wearing sandals, walked into the lobby of Atari and told the personnel director, who was startled by his unkempt hair and attire, that he wanted the job and that he wouldn't leave until they hired him.

Surprisingly, he got the job after a brief interaction with the company's chief engineer who described him as "very intelligent, enthusiastic, [and] excited about tech". He was later assigned to work with an engineer named Don Lang.

The next day Lang furiously complained to his boss: "This guy's a goddamn hippie. Why did you do this to me? And he's impossible to deal with". At the time, Steve Jobs had clung to the belief that his fruit-heavy vegetarian diet would prevent not just mucus but also body odor, even if he didn't use deodorant or shower regularly. It turned out to be a flawed theory!

Lang and others wanted Jobs out, but their boss worked out a solution. "The smell and behavior weren't an issue with me," the boss said. "Steve was prickly, but I kind of liked him. So, I asked him to go on the night shift. It was a way to save him." Jobs would come in after Lang and others had left and work through most of the night.



Even though isolated, Jobs became known for his brashness. On those occasions when he happened to interact with others, he was prone to informing them that they were 'dumb'. "The only reason I shone was that everyone else was so bad", Steve Jobs recalled.

Of course, as we all know, Steve Jobs went on to co-found Apple and in the process, he revolutionized the world of computers, music, movies, and phones. Steve Jobs died in 2011 but to this day, he is still considered to be one of the greatest (and most controversial) visionary business leaders of our generation.

Highly talented people such as Steve Jobs, are a rare breed and in today's swiftly evolving corporate landscape, organizations world-over are on the look-out for them. These individuals can form the bedrock of any business's prosperity and ultimately drive organisational success. However, if not well managed, they could as well bring the organization to its knees.

This article dives deep into understanding the good, the bad and the ugly, of hiring highly talented people, while analyzing the key related risks, the significance of attracting and retaining them, and the strategies to motivate them.

The Good

With highly talented individuals on board, organizations can navigate through the rough tides of the market, embracing innovation and stimulating growth. And with their remarkable productivity and creativity, they can transform organizations from mediocre to star performers.

These unique individuals can see possibilities where others see challenges and are not afraid to tread the path less travelled. Their inherent curiosity usually drives them to question the status quo and seek better ways of doing things.

Motivated by the thrill of winning, their meaningful questions, varied opinions and disagreements, can force peers and leaders into challenging assumptions. At the end of the day, these 'misfits/rebels', can literally make everyone better and push their organizations forward.

The Bad and the Ugly

Sometimes, stars can actually kill an organization. This could happen when individuals exceptionally deliver on their bottom-line goals, but because of arrogance and big egos, they fail to work with others, while abusing organizational rules. I like to refer to these individuals as "brilliant jerks".

A star's ego can be a dangerous thing. I have seen many talented people letting their ambitions spin out of control. I have seen terrific accountants, bankers, and lawyers get told one too many times that they are irreplaceable, and they start swaggering around to the point that their teams resent them. I have also seen smart and capable individuals come to believe that they are so indispensable that they should not be bound by anything, including the company's policies and procedures.

In other situations, the high achievers tend to want to volunteer for more responsibilities, beyond their stated job

descriptions. They take on more work from their supervisors than they can execute, thus end up not delivering. There's nothing heroic or commendable about taking on too much and then fail to deliver on it.

Also, in my experience, I have observed that small and medium-size organizations - which make up the greater portion of corporate Uganda - often struggle to attract and retain highly talented people due to their limited remuneration packages. These stars usually want to be rewarded for their great performance. Plaques and public recognition have their place. But without money, they will easily leave, and the organization will have to go through the costly, time-consuming hiring process to find their replacements.

Lessons for managers and leaders

Firstly, it's critically important that managers and leaders foster a work environment that can attract and retain highly talented people. I am particularly referring to an environment where people can effectively work together, be well motivated, and grown into leaders.

Secondly, the organization chart should be as flat as possible, with blindingly clear reporting relationships and responsibilities. If you want to manage highly talented people effectively, help them by making sure that the organization chart leaves as little as possible to imagination. It should paint a crystal-clear picture of reporting relationships and make it patently obvious who is responsible for what results.

The organization must tightly align great performance with rewards. The better people perform, the more they should be rewarded. There is hardly anything more frustrating than working hard, meeting or exceeding expectations, and discovering that it doesn't matter to your organization. Even the Nobel prizes come with cash awards!

In addition, to effectively manage highly talented people, the organization must conduct routine and candid performance evaluations. Great performance must be praised while bad behavior must be condemned, and where change fails, the culprits should be shown the door no matter how talented they are.

But when all is said and done,
one irrefutable fact remains: **the
benefits of hiring highly talented
people greatly outweigh those of
hiring mediocre ones!**

THE PERILS OF LIVING ABOVE YOUR MEANS: NAVIGATING THE FINANCIAL TIGHTROPE

AISHA NAKANWAGI

Customer Financial Advisor - NSSF



Imagine a financial landscape where the delicate balance between income and expenditure plays out as a captivating story. We find ourselves in a world where overspending becomes a tempting melody, fuelled by borrowing and dwindling savings—a narrative not confined to the borders of America as shared in the CNBC Your Money Financial Confidence Survey, where more than half, or 58% to be precise, of all Americans are now living pay check to pay check; but this resonates globally, perhaps even worse on the bustling streets of Uganda.

The storyline evolves into a tightrope walk, where individuals, living paycheck to paycheck struggle to maintain their financial balance. Every hard-earned shilling is immediately claimed by bills for utilities, food, clothing, entertainment, and for many, luxuries, to mention but a few, leaving no room for financial breathers.

Let us unpack some of the drivers of this kind of situation.

1. Current consumption based on anticipated future income

It is a common practice for some people to finance their current consumption through borrowing, in anticipation of future income, which could be anticipated performance bonuses, salary increment, or even a donation from a friend. Many a time, they venture into debt for grand vacations or elevated lifestyles.

Unlike a promissory note or invoice financing arrangements, which are legally binding, the former arrangements offer no guarantee for the future income. Consequently, the individual ends up failing to pay the debt if the anticipated income is not realized, running a risk of financial distress.

2. The debt dilemma

Borrowing is usually undertaken to bridge the financing gap, which is the difference between the desired expenditure and the cash on hand or in the bank. A debt can be a very good ally if it is taken with caution and strategic planning. On the contrary, overborrowing or borrowing without adequate capacity to pay can create a crisis for the borrower, causing him or her to live paycheck to paycheck. For example, if one loses a job but with a substantial outstanding mortgage balance, one may find it difficult or fail to meet one's mortgage obligations, resulting in foreclosure by the lender—usually a financial institution!

Another example is a personal loan for special occasions like a wedding, graduation or any other celebration. Since such expenditures have no financial returns, the borrower may not have sufficient liquidity to settle the financial obligation, which arose out of borrowing.

Therefore, careful consideration of repayment capabilities is crucial to avoid long-term financial stress.

3. Spending without a budget

A budget does not only act as a financial roadmap, but it also plays a key role in ensuring disciplined spending. A carefully prepared budget will identify the possible sources and amount of finances available, and the expected expenditure, but most importantly, it helps to identify any possible funding gaps.

On the contrary, spending without a budget is like navigating the seas without a compass; it is difficult to figure out the direction of your destination. Without a budget you may end up spending more than your income, which is characteristic of impulse buying.

However, it is important to note that just having a budget is not sufficient to control impulse buying; it requires self-discipline to stick to your budget every time you make an expenditure decision. Nonetheless, without a budget, you are most likely to spend far beyond your income.

4. Lack of emergency/contingency plan

As unforeseen challenges knock on the door, the absence of an emergency fund becomes a chink in the financial armour. Although there is no amount of preparedness that can prevent every emergency from happening, preparedness minimizes the negative impact of an emergency. Therefore, in terms of financial planning, it is important to make a provision for unforeseeable incidents in the budget.

Let's delve into the risks that this kind of lifestyle leads to. Living above one's means is like walking a perilous financial tightrope—a delicate balancing act that many individuals find themselves attempting. In a world where consumerism often dictates our lifestyles, the allure to spend beyond our earnings becomes an overpowering force. While the immediate gratification of a luxurious lifestyle may seem enticing, the long-term consequences can be severe.

R1: Mounting debt crisis

Living above your means inevitably leads to the accumulation of debt. Borrowing to sustain a lifestyle beyond your income not only results in high-interest payments but also creates a cycle that can be challenging to break. Affected individuals find themselves trapped in a relentless cycle of repayments, sometimes borrowing to pay debts!

Once plunged in a debt crisis, such individuals cannot afford even the necessities of life, becoming destitute, if lucky not to be in prison.

R2: Stress and anxiety

The constant pressure of managing bills, debt, and the fear of financial insecurity can lead to heightened stress and anxiety levels. Mental health suffers as individuals grapple with the consequences of their financial choices, impacting both personal well-being and relationships.

R3: Limited savings and investments

Living beyond your means often leaves little room for saving or investing for the future. Inadequate savings can leave individuals vulnerable to unexpected expenses, emergencies, or economic downturns. The absence of a financial safety net exacerbates the impact of life's uncertainties, making it challenging to weather financial storms.

R4: Strained relationships

Financial strain is one of the major sources of tension in relationships. For example, if the husband is unable to provide for the family in terms of e.g. food, shelter, clothing, school fees for children, etc., this is likely to cause conflict between the wife and the husband, as well as the children. Usually, such a situation leads to breakdown in communication and lack of respect for one another in the family, and in extreme cases, it can lead to break up of the marriage.

R5: Inability to retire comfortably

Failing to live within one's means can have long-term consequences on retirement plans. Without adequate savings and investments, individuals may find themselves unable to retire comfortably, relying solely on government assistance or family support.

How to manage these risks

Mitigating the risks associated with living above your means requires a proactive approach and a commitment to financial responsibility. Here are some of the strategies to help individuals regain control of their finances and live within their means:

i) Create a realistic budget

Develop a comprehensive budget that outlines your income, fixed expenses, and discretionary spending. Be honest about your financial situation and allocate funds wisely. Prioritize essential expenses such as housing, utilities, and debt repayment, and allocate a reasonable amount for discretionary spending. Avoid the tendency of having the budget in your head, write it in a notebook or use apps like Expense Tracker, Easy Budget, as well as MS Excel, which is a good tool for budgeting.

ii) Emergency fund

Establishing an emergency fund is crucial for financial stability. Save a portion of your income in a dedicated savings account to cover unexpected expenses, such as medical bills or car repairs. Having an emergency fund can prevent the need to rely on borrowing or loans when unexpected costs arise. This fund has to be in an avenue that is accessible, for example, a Unit Trust, which pays within 24 hours upon application for your funds. Desist from placing emergency funds in fixed accounts and other instruments that cannot be easily liquidated.

iii) Debt repayment plan

Create a systematic debt repayment plan, prioritizing paying off high-interest debts. Consider consolidating debts for more favorable interest rates or negotiating with creditors for more manageable repayment terms.

iv) Live a lifestyle commensurate with your income

Adopt a lifestyle that allows you to spend less than you earn. Avoid unnecessary expenses; distinguish between wants and needs and avoid succumbing to societal pressure to maintain a certain lifestyle. Living within your means creates room for savings and financial security.

v) Increase income

Explore opportunities to increase your income, such as pursuing a side job, freelancing, or investing in professional development to enhance your career prospects. Supplementing your primary income source can provide additional financial flexibility, as the saying goes, "Never put your eggs in one basket".

vi) Financial education

Invest time in educating yourself about personal finance. Understand the basics of budgeting, investing, and managing debt. There are various resources, including books, online courses, and financial advisors, that can help improve your financial literacy and decision-making. The NSSF Financial Literacy program is a good way to start. Visit Financial Literacy program on the NSSF website. & YouTube channel.

vii) Automate saving

Set up automated transfers to your savings account. Treating savings as a non-negotiable expense ensures that you consistently contribute to your financial goals. This disciplined approach helps build a financial cushion over time.

viii) Avoid impulsive purchases

Practice mindful spending and avoid impulsive purchases. Consider implementing a cooling-off period for significant expenditures to evaluate whether they align with your financial goals. This approach reduces the likelihood of making decisions based on temporary desires.

ix) Take time to analyze your expenses, and negotiate prices where applicable

Review recurring expenses such as insurance, utilities, and subscriptions regularly. Negotiate with service providers for better rates or consider switching to more cost-effective alternatives. Additionally, always endeavor to negotiate

the prices of your purchases, unless in supermarket, where prices are fixed. In Uganda, there is a well-established practice, where traders or service providers add a margin on the actual price for negotiation. These small adjustments can contribute to significant savings over time.

x) Seek professional guidance

It is advisable to seek professional advice if you are investing or making unique purchases, for which you are not knowledgeable about. This minimizes potential losses, which undermine your financial stability.

Professional financial advisors can provide personalized strategies and guidance to help you regain control of your financial situation.

Conclusion

Living above your means is a risky behaviour that can have far-reaching consequences on your financial, mental, and emotional well-being. It requires a conscious effort to break free from the cycle of overspending and prioritize financial health. By adopting prudent financial habits, such as budgeting, saving, and investing wisely, you can navigate away from the risks associated with living beyond your means, and build a more secure and fulfilling future. It's never too late to reassess and make the necessary changes to achieve financial stability and peace of mind.



MANAGING LEGAL & COMPLIANCE RISKS IN BUSINESS: THE IMPERATIVE OF SEEKING LEGAL COUNSEL

LILIAN ARINDA

Associate, H&G Advocates



One of the key risks that every business faces regardless of its nature and size, is legal and compliance risk. Every business is affected by various laws and regulations, right from formation to operation; and failure to fulfill the statutory requirements could result in sanctions and/or penalties, with consequential financial and reputational impact.

Obviously, the larger the business, the greater the compliance risk. The span of activities and the number of stakeholders affected by the operations of a large business are huge and therefore, its compliance obligations become onerous. There are numerous laws and regulations in the country, but interestingly many business owners have no idea about the existence of the laws and regulations that affect their businesses. Unfortunately, they have no defense in ignorance of the law, consequently many have been caught with their pants down and have had to pay heavily for non-compliance. For instance, the companies' registry recently struck off the register over 186,000 companies due to failure to file annual returns.

To avoid the negative consequences of non-compliance, which can sometimes be severe, to the extent of causing the collapse of the business, it is prudent that every business should consider hiring/consulting a lawyer. The Ugandan business environment and legal regime, like any other jurisdiction, has a number of legal and regulatory requirements. The initial stages of business formation, although they possess their own complexities requiring

legal expertise, may be the least complicated aspect of the business development process. The operational phase, depending on the nature of the business, presents different and nuanced challenges. Having a legal expert on board is one of the ways through which a business can smoothly navigate those challenges.

The decision to start a business is often influenced by various factors. For businesses involving two or more people, starting is usually founded on mutual trust. The existence of trust amongst founders cements the initial formation process. The persons arrive at the decision of the form of the business venture they wish to engage in, obtain the necessary certifications and thereafter commence business. Of course, this is the oversimplified version of starting a business. The process can be tedious, depending on the form of the business vehicle and the nature of the business.

Once the business is in place, the founders of the business operate on the understanding of friendship and trust, and that might sustain the business - at least for a while. As the business scales and makes profit, the friendship and mutual partnership of the founders might not be sufficient in sustaining operations and ensuring harmonious dealing among the founders, employees, customers and management. The relationship, especially among the founders, and between the company and employees, needs to be regulated by a legal mechanism to ensure smooth operations.

Various factors may cause a drift in the friendships or mutual partnerships. Divergence of views is also equally likely to arise. For businesses that operate as companies, the founders are distinct from the business, which is regarded as a separate legal personality under the law. That is also bound to affect the dealings amongst the founders of the business.

The founders may, for instance, not appreciate the fact that, much as they are the ones who set up the business, once the business is registered as a company, it is a legal entity/person that is separate from them; it can own property, sue and be sued in its own name. Lack of appreciation of this concept of legal existence of a company, leads to founders/owners failing to separate personal transactions from company/business transactions, among other things.

Besides, in any business, there are legal risks and implications that arise. As already mentioned, even the decision to start a business and the business vehicle to use ought to be informed from a legal standpoint. The law provides various avenues through which individuals can establish businesses, all with their pros and cons. Some of the commonly used business vehicles are companies, partnerships and sole proprietorships. Depending on the type of business a person intends to carry out, seeking legal advice as to the type of business vehicle to use will help grant an understanding as to the benefits and suitability of a particular vehicle.

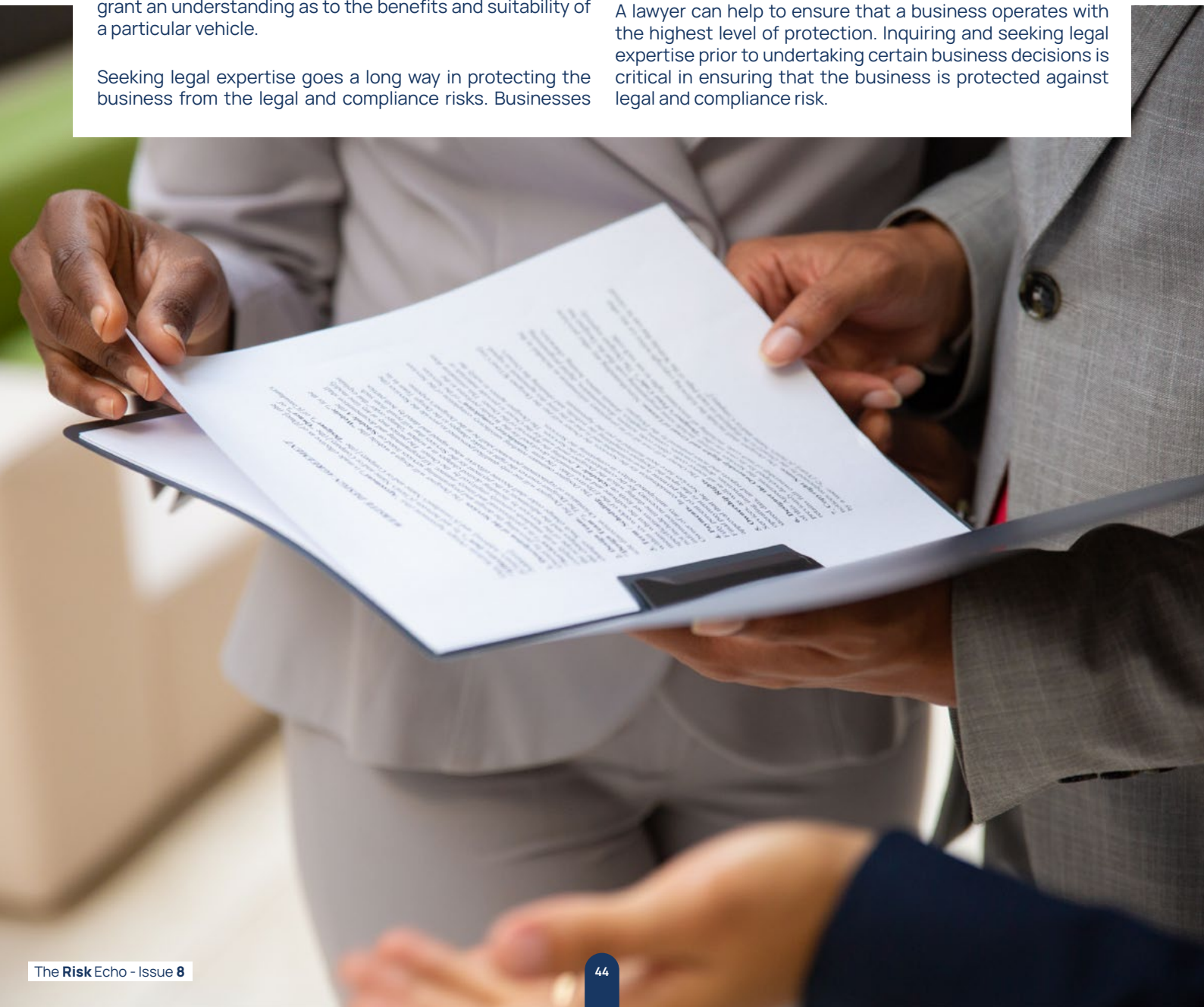
Seeking legal expertise goes a long way in protecting the business from the legal and compliance risks. Businesses

are subject to legal and regulatory requirements. From mandatory filings to mandatory licensing/certifications to reporting. Regulatory requirements always arise because businesses do not operate in a vacuum. While in the short term, noncompliance with the legal and regulatory requirements seems inconsequential, the long-term consequences might be adverse to the business.

Despite the size of a business, compliance provides long term benefits. A quick example is ease of access to financing. Any prudent lender would be hesitant to lend to an individual or a company that is accused of non-compliance with statutory obligations such as tax, social security, mandatory filings, etc. Such an individual or company could be sanctioned or penalized by a regulator, increasing its chances of default.

The day-to-day operations of a business also present legal dilemmas. Certain actions seem insignificant but could potentially have significant ramifications. Whatever it is a business seeks to do; whether contract execution, hiring employees, engaging service providers, making supplies to its customers, acquiring property, etc., all have legal implications. Business relationships are governed by contracts; knowingly or unknowingly, businesses enter into binding engagements.

A lawyer can help to ensure that a business operates with the highest level of protection. Inquiring and seeking legal expertise prior to undertaking certain business decisions is critical in ensuring that the business is protected against legal and compliance risk.



HOW IS THE HYGIENE OF YOUR PERSONALLY IDENTIFIABLE INFORMATION (PII)?

PAULINE KIRE

Offensive Security Tester



Two months ago, at a classy, warm, not too crowded coffee shop in town, I met an elderly woman; very sweet, polite, possibly in her seventies, trying to carry out an online transaction. Although she did not have a clear idea of how to execute the transaction online, by the mere fact that she knew about online transactions and was trying to undertake one, shows that she was more knowledgeable about technology than the average Ugandan woman of that age.

As I graciously offered my help, she reached into her bag and pulled out a pen and an old piece of paper from a tattered notebook. To my astonishment, the paper was filled with account number details, what appeared to be a PIN or a password from here to there, and more. I couldn't help but gasp in disbelief.

After assisting her with the online transaction, I took a moment to educate her about the importance of safeguarding her Personal Identifiable Information (PII). She stared at me like I was a part-time traveller from the future. That's when it dawned on me that there could be many other people, indeed there are, who are like this woman, have no idea of the importance of PII hygiene.

Unveiling PII hygiene - Scrub-a-dub-dub!

First things first, what is PII hygiene? Imagine it as the digital equivalent of maintaining personal hygiene. Just as you wash your hands to stay healthy, PII hygiene is about keeping your sensitive information clean and secure in the digital world.

Defining PII - What is it really?

PII/Personally Identifiable Information sounds fancy, but it's just the stuff that identifies you; well, you! It includes:

- Email addresses (the digital mailbox)
- Phone numbers (your hotline to the world)
- Home addresses (your castle's coordinates)
- Financial info (your digital wallet)
- Social Security numbers (your VIP pass)
- Passwords and PINs (your secret handshake)
- Birthdates (your annual "you're awesome" celebration)
- Your name, gender, height, weight, next of kin, etc.

The risks of scribbling down your PII - spoiler alert: It's not a good idea!

Let's face it; most likely you've all seen someone jotting down their PII on paper, or worse, you have at some point, jotted down your own. But what are the dangers? Think of it as locking your house and leaving the key in the lock!



The risks include but not limited to:

Identity theft: Scammers can exploit your PII to impersonate you before third parties at the expense of your interests.

Financial loss: Unauthorized access to your bank details can lead to financial disaster (say goodbye to that extra avocado toast).

Cyberattacks: Weak PII protection opens the door to hacking and phishing attempts (cyber bad guys never take a day off).

The psychological toll of data breaches - drama unleashed!

A breach of your PII can be emotionally draining. Imagine the shock of discovering your personal life exposed to strangers. The psychological impacts may include:

- **Anxiety and stress:** The feeling of invasion can cause emotional distress (cue the nail-biting).
- **Anger and frustration:** Victims often experience anger at themselves or the perpetrators (grumbling included).
- **Loss of trust:** It can erode trust in digital services, as the online community becomes jittery about online transactions.

When our loved ones are at risk - Superhero mode, activate!

My encounter with the elderly woman left me thinking about my own elderly loved ones. Are they in the same boat? Can they be rescued from potentially disastrous PII practices? It was a wake-up call to extend a helping hand to those who may be vulnerable in the digital age. After all, every superhero has a mission!

Best practices for PII protection - Defend your digital castle!

How can you keep your digital treasure chest secure? Here are some ways for protecting your PII, that even James Bond would be proud of:

1) Memorize sensitive info.

As much as possible, memorize sensitive information, such as passwords, PINs, etc., and stay far away from jotting them down on paper or in any notebooks.

2) Digital vault.

Use secure password managers to store and generate strong, unique passwords (you can't break into Mbuya military barracks with a toothpick).

3) Two-factor authentication (2FA)

Enable 2FA wherever possible, to add an extra layer of security (double trouble for cyber baddies).

4) Shred the evidence

Dispose of physical documents containing PII using a cross-cut shredder

5) Privacy filters

Shield your screens from prying eyes in public places.

6) Regular checkups

Monitor your accounts for suspicious activities and changes (detective hat on!).

Conclusion

In the digital age, you are the guardian of your digital realm. By practicing good PII hygiene, you not only protect yourself but also contribute to a safer online community. Remember, a clean digital slate is a happy one! With these insights, you can navigate the digital world confidently, knowing your PII is secure. Stay vigilant, stay informed, and stay safe in this ever-evolving digital landscape.



ENTERPRISE RISK MANAGEMENT IN A DIGITAL SPACE

MUBIRU ISRAEL

Head of Risk, NIC General Insurance



In today's fast-paced and interconnected business landscape, companies face an unprecedented array of risks emanating from the ever-changing business environment, including the digital space. In this article, I try to show how Risk Managers can address the risks effectively, especially in the digital space.

So, what's digital space? According to Wikipedia, this refers to the virtual environment created using digital technologies, primarily the internet and computer-based systems. It encompasses the online realm, where digital information, data, and communication occur. Digital space is not confined to a physical location but rather represents the interconnected network of digital platforms, that is, websites, applications, and electronic communication channels. Over time, digital space has evolved, and many companies have adopted various technologies.

Digital space and interconnectedness, while providing numerous benefits and opportunities, also introduce various risks and challenges. As individuals, businesses, and societies become more interconnected through digital technologies, it's essential to be aware of the potential risks. Here are some key risks associated with digital interconnectedness.

a) Cyber threats

With increase in the development of applications for use in the digital space, there is equally increase in cyber threat. According to a Deloitte Center for Controllershship poll, during the past 12 months (2023), 34.5% of polled executives reported that their organizations' accounting and financial data were targeted by cyber adversaries. Within that group, 22% experienced at least one such cyber event and 12.5% experienced more than one." And "nearly half (48.8%) of C-suite and other executives expect the number and size of cyber events targeting their organizations' accounting and financial data to increase in the year ahead.

One way this risk materializes is through malicious software developed to compromise systems, leading to corruption of data, denial of service, data breaches, disclosure of confidential information, and the consequential financial loss, as well as reputation damage, as explained below:

i) Data privacy concerns

The digital space if not safeguarded, can be exploited by hackers to gain unauthorized access to customer personal data, leading to privacy violation and the associated litigations and reputation damage. The motive of the hackers in most cases is financial, whereby, they ask for a ransom, usually in millions, if not billions of bitcoins. For example, in May 2021, Colonial pipeline fuel distributor's business was disrupted by the ransom attack caused by the Darkside gang. According to an article on the BBC website, <https://www.bbc.com/news/business-57178503>, although initially the CEO had refused to pay, he eventually gave in, and the company paid US \$ 4.4 million to the crooks.

If you fail to meet their ransom demands, they can release the information to the public, leading to lawsuits for breach of data privacy. According to [softwaresecure.com](https://www.softwaresecure.com), Marriott International was fined \$23.8 million by the General Data Protection Regulation (GDPR) for a data breach that exposed the personal information of 339 million guests.

ii) Manipulation and deception

With social engineering, such as phishing in its various forms (email phishing, spear phishing, vishing, smishing and whale phishing), individuals can be tricked into revealing sensitive information or performing actions that compromise data security. This can also be done using deep fakes, where creation of realistic but fabricated audio, video, or text content are used to deceive or manipulate individuals and organizations.

Once the hacker obtains the information, he/she can use it to penetrate your systems, with the consequences mentioned above.

b) Online harassment and cyberbullying

A lot of individual information is shared online, this could be through job applications, social media platforms in form of networking, etc. The increased connectedness can contribute to online abuse, harassment, and cyberbullying, affecting individuals' mental health and well-being. In mid-January 2024, Tylor Swift woke up to find the social media filled with explicit AI images of herself. This impacted her brand image, and she complained to the x.com (former twitter) to have them removed. The originator was located and will be facing the arm of the law.

c) System downtime

The digital space is characterized by system down times, which affect business operations and cause customer dissatisfaction. I have no doubt that anyone reading this article, who has an ATM card, has ever gone to an ATM to withdraw or deposit money and found that the system was off. It is so frustrating, especially when the transaction is urgent, and the banks are closed for a weekend or a public holiday. Failure of critical infrastructure could have widespread consequences such as business continuity issues, resulting in customer dissatisfaction.

d) Regulatory compliance challenges

Digital space technologies face rapid changes, these changes come with changes in regulations since regulators and authorities are not relenting. Adapting to evolving data protection and privacy regulations can pose challenges for organizations operating in a digital landscape.

e) Supply chain risks

Organizations interconnected through supply chains may face risks if a third-party vendor or partner experiences a cyber-attack.

The rise and simplification of technology, increased connectivity, and the widespread adoption of digital processes, have transformed the business landscape, bringing both opportunities and challenges to enterprise risk management (ERM).

To effectively navigate this ever-changing digital space, enterprises must enhance their risk management frameworks. Therefore, let's explore how existing ERM frameworks can be adapted to address the dynamic risks associated with the digital era:

i) Understanding the digital landscape

The first step in effective enterprise risk management is to understand the context in which the organization operates, that is processes, systems, products, policies, procedures, laws and regulations, etc, from which risks emanate.

The digital space introduces new dimensions of risk, including cybersecurity threats, data breaches, regulatory compliance challenges, and the rapid evolution of technology. Failure to understand the changing landscapes, makes the traditional ERM frameworks struggle to keep pace with the speed of change in this environment.

ii) Integration of technology into enterprise risk management

To effectively navigate the digital space, organizations need to integrate technology into their ERM frameworks. This involves leveraging advanced analytics, artificial intelligence (AI), and machine learning to identify, assess, and mitigate digital risks. Automated risk monitoring tools can provide real-time insights into emerging threats, enabling organizations to respond proactively; for example, to detect and reduce fraud, HSBC has heavily invested in AI for anti-money laundering to strengthen controls within that process.

iii) Holistic approach risk management

A successful ERM framework in the digital era must adopt a holistic approach to risk assessment. Instead of focusing solely on financial and operational risks, organizations need to consider the broader spectrum of digital risks, including reputational damage, brand integrity, and the potential impact on customer trust. This requires a shift in mindset from traditional risk silos to a more integrated and comprehensive risk management strategy.

iv) Cybersecurity at the core

Given the escalating frequency and sophistication of cyber threats, a robust cybersecurity strategy should be at the core of any ERM framework in the digital age. This includes regular vulnerability assessments, proactive threat intelligence gathering, and the implementation of robust security measures. Collaboration between the ERM and IT teams, and cybersecurity experts is crucial to developing a resilient defense against digital threats.

v) Agility and flexibility

The digital space is characterized by rapid changes; organizations need to build agility and flexibility into their ERM frameworks. Traditional and static risk management approaches may prove ineffective in the face of dynamic digital risks. Regular reassessment of risk profiles, scenario planning, and the ability to adapt quickly to emerging threats, are essential components of a modern ERM framework.

vii) Regulatory compliance

The digital space is subject to an ever-evolving regulatory landscape. ERM frameworks must be designed to accommodate these changes and ensure compliance with data protection laws, industry standards, and other relevant regulations. Organizations need to stay informed about regulatory developments and adapt their risk management practices accordingly.

viii) Employee training and awareness

Human factors play a significant role in digital risk management. Enterprises should invest in employee training programs to enhance awareness of cybersecurity best practices and foster a culture of risk awareness. Employees should be considered as both potential vulnerabilities and key components of the defense against digital threats.

Conclusion

Navigating the ever-changing digital space requires a proactive and adaptive approach to risk management. By integrating technology, adopting a holistic risk assessment, prioritizing cybersecurity, promoting agility, ensuring regulatory compliance, and enhancing employee awareness, organizations can fortify their ERM frameworks against the challenges posed by the digital era. As digital risks continue to evolve, enterprises must evolve their risk management strategies to stay resilient in the face of an ever-changing landscape.



PUZZLE ISSUE NO.8

1	20	21		22	23	24	25		26
2				3				27	
4			28		5				
6			7			8			
9		29			10				
		11					12	30	
13	31				14	32			
15			33	34		16			35
			17		36				
18							19		

DOWN

1. A lexical token in computing that names the language's entities, 10
10. The term notifies the recipient that something will be happening by the end of the workday, abbr.3
20. A continuous area or expanse which is free, available,5
21. Make a choice from a range of possibilities,3
22. In Medieval Latin means "in the year of the Lord",abbr.2
23. The evergreen shrub, 3
24. A short piece of writing on a particular subject,5
25. A person, plant, or animal that is descended from a particular ancestor,10
26. To show, prove, or state that something is true or real,6
27. An Agency mandated to facilitate the Government's goal of achieving rural electrification, abbr.3
28. The exchange of value for money, 4
29. Coming after all others in time or order, 4
30. Office of Equity and Inclusion, abbr.3
31. Expressing the situation of something that is or appears to be enclosed or surrounded by something else, 2
32. Expressing hesitation or a pause in speech,2
33. A body that reviews and sets electricity tariffs, and other terms of supply of electricity, abbr.3
34. Memory bank where a computer stores data it needs to retrieve quickly, abbr.3
35. Free of all charges or deductions,3
36. A subject designed to develop motor skills, knowledge, and behaviours for physical activity and physical fitness, abbr.2

ACROSS

1. Far away; distant places, buildings, or people; remote,8
2. Judicial official; Uganda abbr.,3
3. Leave say a place, causing it to appear empty; disolate,6
4. Eats: Light food or snacks,4
5. A useful or valuable thing or person,5
6. The state is the 28th-largest and 9th-most populous of the United States, abbr.2
7. Expressing the time when an event takes place,2
8. Accreditation Commission for Audiology Education -USA, abbr.4
9. Communicate information to someone in spoken or written words,4
10. A globular organ in humans ,vertebrate animals etc.,3
11. A combining form meaning "air",4
12. Used to give a negative response,3
13. Financial Information System, abbr.3
14. A slang meaning "guy" or "man.", 4
15. In the midst,5
16. Chief in size or importance,4
17. Strike (a hard surface) with a series of rapid audible blows, especially in order to attract attention,3
18. To give (someone or something) a new name,6
19. The period between the beginning and end of a procedure, abbr.3

SOLUTION TO ISSUE NO. 7

A	C	T	I	O	N		P	A
T	A	C	T		O	V	E	R
T	L	P		C	R	O		R
A	M		E	N	T	I	R	E
C	E	R	M		O	D	E	A
K	R	I		U	N		I	R
E		D	E	A		A	T	S
R	I	D	D	I	N	G	S	
S	O	L	E		O	A		F
	N	E		S	N	I	P	E
A	S	S	U	R	A	N	C	E



The future you aspire to matters, guard it.

Report employers who do not pay your contributions to recover your savings with interest.

Visit www.whistleblower.nssfug.org
to whistle blow or call 0800 286 773.



