The RiskEcho

ISSUE 9 - FEBRUARY 2025

Intriguing Insights

NSSF
a better life

THE RISK ECHO

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

I take this opportunity to wish you a happy 2025. It is my prayer that this year brings great tidings to you. I am delighted to have crossed over to 2025, and I congratulate you for making it to this point in time.

At the Fund, 2024 was a great year because this is the time we launched the SmartLife Flexi product, which has given our existing members and the public an opportunity to voluntarily save in order to enhance their financial stability in the future.

The SmartLife Flexi product is a voluntary goal-based saving plan that enables you to save for a defined goal and period of your choice. It empowers you to choose how much, when and for how long to save, with a minimum of UGX 5,000. After an initial period of 12 months from the time of enrolment, you can withdraw part or all the savings without any penalty. The other key important feature of this product is the return on investment, which is computed daily, reflecting the benefit of compounding.

SmartLife Flexi offers an engaging experience with our members through digital goal-based wallets with inbuilt tools to enable the members keep track of their savings and achieve their life aspiration.

All income earners aged 16 years or above, both nationals (in Uganda and abroad), and non-nationals with valid identifications, are eligible to contribute to this product.

That aside, as usual, in this nineth issue of The Risk Echo, we bring you a variety of articles for your reading pleasure, ranging from technical issues including AI (Artificial Intelligence), phishing, and behaviour issues such as the role of human behaviour in risk management, etc.

Don't miss an interview with Mr. Benoni Katende, the Chief Technology & Enterprise Solutions Officer, talking about how AI is driving efficiency at the National Social Security Fund.

Edward Senyonjo
Chief Risk Officer - NSSF

CONTENTS

INTERVIEW: HOW AI IS DRIVING EFFICIENCY AT THE NSSF

BENONI KATENDE

Chief Technology & Enterprise Solutions Officer (CTESO) , NSSF

The Risk Echo was privileged to secure an interview with the Chief Technology & Enterprise Solutions Officer (CTESO) at the National Social Security Fund, Mr. Benoni Katende, to talk about how the Fund is leveraging AI to drive efficiency.

Mr. Katende, for the interest of our readers, can you introduce yourself in a few sentences.

My name is Benoni Katende, but most people call me Ben. I'm a firm believer in the God of Abraham, Isaac, and Jacob. Professionally, I'm a tech enthusiast and a nature lover—I'm fascinated by innovation and the beauty of the natural world.

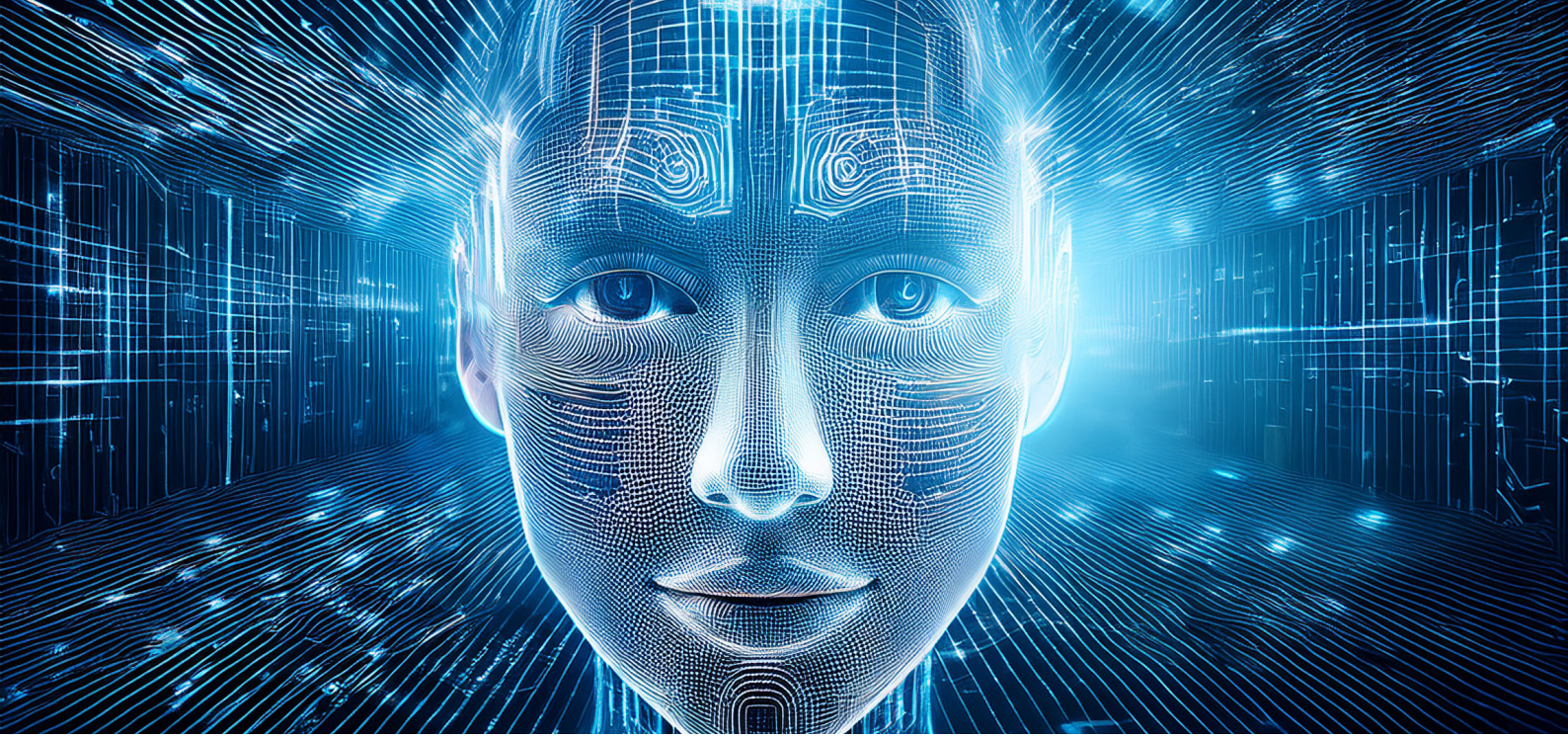
As the Chief Technology and Enterprise Solutions Officer, what is your role at the Fund?

My core responsibility is to oversee technology and data strategies at the Fund. This involves ensuring that all our systems run smoothly, and that we continuously innovate to enhance the experience of both our internal and external customers.

Technology is a double-edged sword; it can make or break you. How is it making or breaking you at the Fund?

Our approach to technology is built on three pillars: Convenience, Cost, and Cognizance. Essentially, we use technology to drive innovation by making processes faster, more cost-effective, and more efficient. It also allows us to broaden our service offerings and reduce complexity.

However, the more we expand our technology footprint, offering self-service options and integrating with numerous third parties, the more we expose ourselves to potential cyber risks.



Fortunately, we have robust processes in place to manage these risks. In short, while technology can bring significant threats, it also provides immense benefits that far outweigh the drawbacks, provided we remain vigilant.

AI is the in-thing in the tech space today; to a lay person, how do you define AI?

Artificial Intelligence (AI) refers to computer systems or machines that can mimic certain aspects of human intelligence such as learning, reasoning, and decision-making. While humans possess natural intelligence, machines rely on algorithms and data to exhibit what we term 'artificial intelligence.'

Is the Fund using AI and in which areas?

Absolutely. AI powers multiple applications within the Fund, including:

- Benefits applications
- Benefits processing
- Customer service quality evaluation
- Application development
- Security incident analysis

Can you share specific examples of how AI is being used to drive efficiency in the Fund?

Certainly. Here are a few examples:

Statement Cleaning Process: AI helps streamline data for benefits processing.

Benefits Application: Our digital and online forms (web and app) use AI for customer authentication.

Financial Literacy System: AI enhances personalized learning experiences.

Call Center Quality Analysis: We use AI to assess and improve customer service interactions.

Doxa (Internal AI Agent): An AI-powered chatbot that assists internal staff with inquiries.

Wellness App: Uses AI for calorie identification and related health features.

How do you see the future of AI in the workplace, particularly in the NSSF?

AI has the potential to revolutionize society, much like the advent of fire, electricity, and the internet. Prominent tech leaders, like Sundar Pichai (Google) and Demis Hassabis (DeepMind), have highlighted how AI may soon match human-level intelligence across many domains.

For us at the Fund, AI could theoretically handle up to 95% of our current operations; everything from automating routine tasks to enhancing strategic decision-making. How we apply AI will ultimately depend on our organizational strategy, ensuring we maintain a balance between efficiency gains and responsible deployment.

What strategies do you have in place to mitigate risks associated with AI, such as data breach, over-reliance on automation, ethical dilemma etc.?

The most effective strategy is awareness and education. We focus on equipping our staff with AI-related knowledge, so they understand both the benefits and potential pitfalls. AI is being deployed in multiple units and integrated into various processes, as seen in the cases mentioned earlier.

Ultimately, just as every department incorporates risk management or financial management into its core responsibilities, we believe there should be a dedicated focus on AI implementation and governance. This includes setting guidelines, monitoring usage, and regularly auditing AI's impact to ensure we remain aligned with ethical standards and security best practices.

INTERNATIONAL PROPERTY AWARDS DEVELOPMENT
BEST RESIDENTIAL DEVELOPMENT AFRICA
Solana Lifestyle & Residences by The National Social Security Fund, Uganda
2021-2022

AFRICAN PROPERTY AWARDS DEVELOPMENT
★★★★★
BEST RESIDENTIAL DEVELOPMENT UGANDA
Solana Lifestyle & Residences by The National Social Security Fund, Uganda
2021-2022

AFRICAN PROPERTY AWARDS DEVELOPMENT
★★★★★
BEST MIXED USE DEVELOPMENT UGANDA
Solana Lifestyle & Residences by The National Social Security Fund, Uganda
2021-2022

Invest in a new way of living this year

PHASE **ONE**
NOW SELLING

10%
Initial deposit to lock-in your unit

40%
Cumulative payment to take possession of your unit

No interest on the due payments

Move into a home deserving of your aspiration in a new sanctuary of smart living.

Now starting from

$142,000*

Buy your dream home today

Visit **www.solanalifestyleandresidences.com**
or call **+256 776 610 612 / +256 778 451 008**
+256 702 762 315 / +256 781 583 494

LIVE • WORK • PLAY • SHOP
An award winning development by NSSF Uganda.

NSSF a better life | SOLANA LIFESTYLE & RESIDENCES

INTEGRATING ESG IN RISK MANAGEMENT

A STRATEGIC IMPERATIVE FOR MODERN BUSINESSES

ISRAEL MUBIRU
Head of Legal, Risk and Compliance, AAR

Environmental, Social, and Governance (ESG) factors are no longer just buzzwords, they have become critical components of a comprehensive risk management strategy. As the world faces increasing environmental challenges, rising societal expectations, and increased corporate governance scrutiny, integrating ESG into risk management frameworks has moved from a nice-to-have to a must-have for businesses seeking long-term sustainability.

In this article, I explore the importance of ESG in modern risk management, how to integrate it effectively, and the benefits of doing so.

Understanding ESG and Its Impact on Risk Management

Environmental factors refer to a company's impact on the planet, including its carbon footprint, resource consumption, waste management, and adherence to environmental regulations, among others. These elements have direct implications for operational risks, regulatory compliance, and reputation management.

Social factors relate to how a business manages relationships with various stakeholders such as employees, suppliers, customers, and communities. Issues like labour practices, human rights, diversity and inclusion, and product safety, can be sources of significant risks such as legal disputes, reputation damage, low workforce productivity, inter-alia.

Governance involves the systems and processes that ensure corporate transparency, ethical decision-making, and accountability. It includes board structure, executive compensation, auditing processes, shareholder rights, and risk management. Weak governance practices can result in financial, legal, and reputational risks.

As global attention intensifies on these issues, integrating ESG factors into risk management enables organizations to not only identify emerging risks but also create more resilient and sustainable strategies.

Why Integrating ESG is Crucial for Risk Management

i) Regulatory Pressure and Legal Compliance

Governments worldwide are increasingly enacting regulations around ESG-related practices. For example, the European Union's Corporate Sustainability Reporting Directive (CSRD) and the U.S. Securities and Exchange Commission's (SEC) proposed climate disclosures have made it clear that companies must disclose their ESG risks. Failing to adhere to these regulations exposes companies to fines, legal action, and reputational damage.

ii) Need to safeguard company brand/reputation

Consumers, investors, and employees are becoming more discerning about corporate ethics. A failure to act responsibly on ESG issues can lead to a damaged reputation, loss of consumer loyalty, and the potential for public backlash. Conversely, a positive ESG record can differentiate a company in the marketplace and improve stakeholder relations.

ii) Operational and Supply Chain Risk

ESG issues can affect supply chains in several ways, from climate-induced disruptions (e.g., extreme weather events) to human rights abuses within supply chains. Managing ESG risks means anticipating and mitigating potential disruptions, enhancing operational efficiency, and ensuring continuity in the face of environmental and social challenges.

iii) Financial Risk

ESG issues directly influence a company's financial performance. Poor environmental practices may result in costly penalties, while governance failures (like fraud or corruption) can lead to significant financial losses. Conversely, businesses that manage ESG risks effectively may benefit from lower capital costs, higher investor confidence, and improved long-term profitability.

iv) Investor Demands and Market Trends

Institutional investors and stakeholders are increasingly prioritizing ESG criteria when making investment decisions. Many investment funds now follow ESG-centric mandates, and companies that fail to meet these expectations may see a decline in investment. By integrating ESG into risk management, companies are better positioned to attract and retain capital.

Steps to Integrate ESG into Risk Management

a) Assess ESG Risks Across the Enterprise

The first step in integrating ESG into risk management is identifying potential risks across all ESG categories. This includes:

- Conducting a materiality assessment to determine which ESG issues are most relevant to your business.
- Mapping out risks by considering factors like climate change, supply chain disruptions, social unrest, data security, and governance failures.
- Reviewing current policies and practices in light of evolving ESG criteria.

b) Embed ESG into Governance Structures

Effective ESG risk management requires strong leadership and clear accountability. This can be achieved by:

- Appointing a Chief Sustainability Officer (CSO) or ESG Committee responsible for overseeing ESG strategy.
- Ensuring the board of directors possesses ESG expertise to make informed decisions on matters related to ESG.
- Aligning executive compensation with ESG performance to incentivize the right outcomes.

c) Develop ESG-Centric Risk Frameworks

Traditional risk management models need to be reviewed to include ESG factors. This can be done by:

- Incorporating ESG metrics into the enterprise risk management (ERM) framework.
- Identifying both short-term and long-term ESG risks, and evaluating their potential financial, operational, and reputational impacts.
- Using scenario analysis to forecast how ESG issues could affect business performance under different conditions (e.g., regulatory changes, climate change, or social movements).

d) Implement ESG Performance Metrics and Reporting

Measuring ESG performance is crucial for understanding how well a company is managing these risks. Establish clear metrics for monitoring ESG risks, such as:

- Environmental impact (carbon emissions, water use, waste generation)
- Social factors (employee turnover, community impact, diversity and inclusion)
- Governance factors (board diversity, executive pay, audit integrity)

Additionally, regularly report these metrics to stakeholders (investors, regulators, customers) using recognized ESG reporting standards like the Global Reporting Initiative (GRI) or Sustainability Accounting Standards Board (SASB).

e) Engage Stakeholders

ESG risks affect multiple stakeholders, including investors, employees, customers, and communities. Engage these groups in the risk management process to:

- Understand their concerns and expectations.
- Build partnerships to mitigate ESG risks (e.g., collaborating with suppliers on sustainable practices).
- Promote transparency and trust through open communication about how ESG risks are being managed.

f) Establish a Response Plan for Emerging Risks

ESG risks evolve over time, and some may emerge unexpectedly (e.g., a sudden regulatory change, a natural disaster, or a social movement). Having a proactive response plan that includes:

- Crisis management protocols.
- Flexibility in adapting business practices to changing ESG conditions.
- Regular review and update of risk management processes to ensure readiness.

g) Monitor and Review ESG Risk Management

Regular monitoring and evaluation are essential to ensure that ESG risks are being effectively managed and mitigated. This can be done through:

- Internal audits of ESG compliance.
- Continuous monitoring of ESG-related developments in the industry and in global markets.
- Reviewing ESG performance reports to identify areas for improvement.

Conclusion:

As ESG considerations are becoming more critical in today's business landscape; integrating them into risk management is no longer optional—it's a strategic imperative. Companies that actively manage ESG risks are better positioned to thrive in an increasingly complex and interconnected world. By embedding ESG into risk management frameworks, businesses can safeguard their future, meet stakeholder expectations, and contribute positively to the global community well-being.

SAFEGUARDING CHILDREN ONLINE:

THE ROLE OF PARENTS IN A DIGITAL WORLD

CHRISTINE HILDA NAMUDDU

Information security & Data Protection Manager, NSSF

The internet presents numerous benefits for children, offering them access to educational tools, entertainment, and social interactions. However, these opportunities are accompanied by potential risks, such as cyberbullying, exposure to harmful content, online predators, and privacy concerns. As children become increasingly adept with technology from a young age, it's essential for parents to actively guide their online safety. This responsibility extends beyond mere supervision, it includes establishing protective measures and maintaining an open, ongoing conversation about responsible internet use.

Recognizing Online Risks to Children

Children, with their natural curiosity and innocence, are especially susceptible to a variety of online dangers, including but not limited to;

1. Cyberbullying

Harassment can happen through social media, messaging apps, and gaming platforms, often causing significant emotional distress to children. A Malaysian TikTok user, Esha, tragically took her own life after being a victim of online harassment. Rehtaeh, from Halifax, Nova Scotia, was a victim of cyberbullying and sexual assault. After a photo of her assault circulated online, she was continually harassed by her peers, eventually leading to her suicide. The foregoing gives a few of the many examples of cyber bullying and its effects on the victims.

2. Access to Inappropriate Content

Without proper safeguards, children may stumble upon violent, sexually explicit, or otherwise unsuitable material for their age. For instance, reports have shown that children often encounter sexual content or violent material through platforms like YouTube, TikTok, or gaming environments. A notable case in 2023 involved children as young as eight accessing explicit material through popular social media apps despite platform rules that claim to restrict such content. For example, a survey by CyberSafeKids found that over 80% of children between the ages of 8 and 12 had social media profiles, many without proper parental control or oversight.

3. Online Predators

Predators may use the anonymity of the internet to connect with children via social media, chat rooms, or online games. Breck, a 14-year-old, was lured by Lewis Daynes, a young man he met through an online gaming community. Despite warnings from his parents, Breck continued communicating with Daynes, who manipulated him emotionally, isolating him from family and friends. The relationship tragically ended in Breck's murder after a secret meeting arranged by Daynes. In 2022, according to the Online Sextortion of Minors report, more than 700 cases of online financial sextortion of minors were reported, targeting mostly teenage boys (14-17 years old).

4. Privacy and Data Safety

Children might unknowingly share personal details like their location, school, or photos, risking their safety or even leading to identity theft. In 2023, TikTok was fined US $368 million by European Union for failing to protect children's privacy. It was discovered that TikTok set children's accounts to "public" by default, allowing anyone to access their content. Also in 2022, YouTube was fined US $170 million for collecting data on children under 13 without their parents' consent. These are the few examples of known breaches to the privacy of children.

5. Addiction and Excessive Screen Time

Spending too much time on social media or gaming can lead to addictive behaviours, potentially impacting a child's mental health and overall development. A 2024 survey conducted by a paediatric health organization revealed that 60% of children aged 8–12 had their own smartphones, with many using them for more than 5 hours daily.

The Role of Parents in Ensuring Online Safety

Parents are the first line of defense when it comes to protecting children online. While technology continues to evolve, there are several strategies and tools parents can use to safeguard their children:

1. Setting Up Parental Controls

One of the most effective ways to manage a child's online activity is by implementing parental control tools. These tools can filter, monitor, and limit internet usage across devices.

Web Filtering: Parental control software can block access to inappropriate websites, ensuring children don't stumble upon harmful content.

App Restrictions: Parents can restrict access to specific apps or features on their children's devices (e.g., limiting access to social media or online games).

Screen Time Management: Many parental control tools allow parents to set daily or weekly limits on how much time their children spend online.

Some popular parental control tools include Net Nanny, Qustodio, Kaspersky Safe Kids, and built-in options like Google Family Link and Apple Screen Time.

2. Educating Children About Online Risks

Beyond technical solutions, it is critical for parents to have ongoing conversations with their children about the risks they might encounter online. Empowering children to recognize and respond to online threats is key to their safety.

Explain Cyberbullying: Help children understand what cyberbullying looks like and encourage them to report any inappropriate behaviour, whether they are the target or witnessed it.

A Malaysian TikTok user, Esha, tragically took her own life after being a victim of online harassment.

Teach Privacy Protection: Educate children on the importance of not sharing personal information online, even with people they think they know. This includes limiting what they share on social media and avoiding online interactions with strangers.

Inappropriate Content: Discuss what constitutes inappropriate content and encourage children to come to their parents if they encounter something that makes them uncomfortable.

These conversations should be regular and adapted as children grow and their online experiences change.

3. Monitoring and Supervision

While parental controls can help, parents should also stay actively involved in their child's online activities. Monitoring doesn't have to feel intrusive, there are ways to do this while still fostering trust.

Review Browsing History: Periodically checking your child's browsing history or the sites they visit can provide insight into their online behaviour.

Set Up Usage Agreements: Establish clear rules and boundaries for online activities. For example, agree on which websites they can visit, who they can communicate with, and the amount of screen time they are allowed each day.

Be Present: For younger children, consider placing computers or tablets in common areas of the house so that internet use is more visible. For older children, find ways to stay involved in their online world, such as discussing the apps or games they use.

4. Setting Age-Appropriate Boundaries

Not all children need the same level of online freedom. Parents should tailor their approach based on their children age and maturity level:

For Young Children (under 10): Focus on limiting internet access to age-appropriate content. Use heavy parental controls, limit screen time, and ensure they don't have unsupervised access to devices.

For Pre-Teens (10-13): This is the age when children start exploring social media and online gaming. Continue using parental controls but also focus on conversations about privacy and safe online behaviour.

For Teenagers (13-18): While teens require more independence, parental involvement remains important. Loosen some restrictions but continue to monitor their activities, and guide them on responsible online behaviour, privacy management, and digital reputation.

5. Encouraging Open Communication

It's essential for children to feel comfortable coming to their parents if they experience something unsettling online. A punitive approach may discourage children from sharing their concerns, leading them to hide their online activities.

Create a Safe Space for Discussion: Let your child know that if they come across something inappropriate or dangerous online, they won't be punished for reporting it.

Be Approachable: The more open and supportive parents are about digital safety, the more likely children will seek help when they need it.

6. Staying Updated on Technology Trends

The digital world changes quickly. As new platforms, apps, and technologies emerge, parents need to stay informed. By understanding the latest trends, from new social media platforms to the risks associated with apps like TikTok or Snapchat, parents can better guide and protect their children online.

7. Leveraging Technology for Protection

As much as the internet can be a dangerous space, it also offers solutions for protection. Parents should make use of the tools available to them:

ANTIVIRUS & ANTI-MALWARE SOFTWARE:

Installing these on all devices used by children can help prevent malware, phishing, and other cyberattacks.

VIRTUAL PRIVATE NETWORKS (VPNS):

VPNs provide an extra layer of security by hiding the child's internet activity and protecting them from potential hackers.

CHILD-SAFE BROWSERS AND SEARCH ENGINES:

Using kid-friendly browsers likeKidRex or settings like Google SafeSearch helps filter out inappropriate search results.

Conclusion:

The internet is a double-edged sword that requires balancing freedom and safety for children. On the one hand, it offers incredible learning opportunities and connections, on the other, it exposes them to serious risks. As parents, the goal is not to stifle their online experiences but to empower them to navigate the digital world safely and responsibly.

Implementing parental controls, having regular conversations about online risks, and staying informed about new digital trends, are all critical steps in protecting children online. By fostering an environment of trust and responsibility, parents can ensure their children enjoy the benefits of the internet without falling prey to its dangers.

Proverbs 22:6 Train up a child in the way he should go, and when he is old he will not depart from it.

Introducing

Smartlife Flexi®

a better way to save

Because the **Smart**life **Flexi** plan lets you start saving with **as low as Shs 5,000.**

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

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

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

*Terms and conditions apply.

NSSF
a better life

THE ROLE OF EXPOSURE MANAGEMENT IN RISK PREVENTION

HOPE VICTORY SHABA
Information Security Specialist - NSSF

RIP- Your are dearly missed; we deeply appreciate your valuable contribution to this publication

Managing exposure in systems security is like playing an endless game of whack-a-mole; instead of pesky rodents, you're facing an ever-evolving swarm of cyber threats. For corporate professionals, particularly those in cybersecurity, exposure management has become crucial for maintaining an organization's security and integrity. Whether you're the Chief Information Security Officer (CISO) of a multinational corporation or the tech expert in a growing startup, understanding exposure management can save you from potential headaches—or worse, a catastrophic security breach.

What Is Exposure Management?

Exposure management is an evolved form of vulnerability management. It goes beyond merely identifying technical vulnerabilities by integrating these with the business context, offering a comprehensive view of an organization's risk landscape. This approach prioritizes risks based on their potential impact on critical business functions, ensuring that the most significant threats are addressed first. By connecting technical data with the organization's risk appetite, exposure management helps pinpoint areas where the business is most susceptible to attacks, focusing on vulnerabilities that could lead to substantial losses.

This holistic approach also includes third-party risks, recognizing the potential vulnerabilities introduced by external vendors, partners, and supply chains. In today's complex business environment, where companies rely heavily on third-party services and products, managing these external risks has become increasingly important. Proactive strategies like inventory management, patching critical vulnerabilities, and enhancing monitoring capabilities are central to reducing both the likelihood and impact of cyberattacks.

Moreover, exposure management is not a static process; it evolves as the threat landscape and your organization's environment change. As new threats emerge and business operations evolve, exposure management must adapt, ensuring that the organization remains protected against the latest risks.

Why Exposure Management Matters

Imagine starting your day with a cup of coffee, only to be interrupted by an alarming message from your IT department about a data breach. It's a scenario no corporate professional wants to face! However, if your organization has a robust exposure management strategy in place, that panic-inducing moment could be significantly mitigated. Without such a strategy, the fallout from a breach could be disastrous, leading to loss of customer trust, legal repercussions, and significant financial loss.

Exposure management isn't just about avoiding disasters—although that's a significant part of it. It's about understanding your risk landscape and making informed decisions about where to allocate resources. Think of it as risk triage. Not every vulnerability needs immediate attention, but those with the potential to cause catastrophic outcomes must be prioritized. This strategic approach allows organizations to make the best use of their often-limited cybersecurity resources, ensuring they focus on the most critical areas. For example, a vulnerability in a system handling sensitive customer data might be given higher priority over a less critical system vulnerability. By adopting an exposure management framework, organizations can better align their cybersecurity efforts with their overall business goals, ensuring that the areas of highest risk are addressed first.

Exposure Management vs. Vulnerability Management

To fully grasp the importance of exposure management, it's essential to distinguish it from traditional vulnerability management. While both concepts are related, they differ significantly in scope and approach.

Vulnerability management focuses on identifying, classifying, and mitigating technical vulnerabilities within an organization's IT infrastructure. It involves regular scanning, assessment, and patching of systems to ensure known vulnerabilities are addressed. However, this approach often operates in a narrow scope, focusing solely on technical aspects without considering the broader business context.

On the other hand, exposure management takes a more holistic view. It integrates technical vulnerabilities with business considerations, such as the organization's risk

appetite, the criticality of business functions, and the potential impact of a breach on these functions. This integration allows for a more comprehensive understanding of where the organization is most exposed to risks, enabling better prioritization and more informed decision-making.

In essence, while vulnerability management is about fixing what's broken, exposure management is about understanding what matters most and addressing the most significant risks first. It's a proactive approach that considers the entire risk landscape, including external factors like third-party risks, and continuously adapts to changes in the threat environment.

Steps for effective exposure management

1. Leverage Threat Intelligence

Integrating threat intelligence into exposure management allows businesses to stay ahead of potential risks by providing real-time insights into emerging threats. To achieve this, do the following:

Identify New Threats: Continuously monitor the latest cyber threats and attack vectors to adjust your exposure management strategies accordingly.

Assess Risk Impact: Evaluate how new threats could impact critical assets, enabling better prioritization of response efforts and resource allocation.

Enhance Incident Response: Assess and improve the organization's ability to respond quickly and effectively to emerging threats with up-to-date threat intelligence.

Inform Strategic Decisions: Use threat intelligence to guide decisions on which vulnerabilities to address first and which third-party relationships to re-evaluate.

2. Management of Third-Party Risks

With increasing reliance on external vendors and partners, third-party risks are a growing concern. To mitigate these risks:

Assessment of Third-Party Security: Evaluate and ensure that vendors and partners meet your security standards to protect sensitive data and systems.

Continuous Monitoring: Regularly monitor third parties for any changes in their risk profile, not just at the beginning of the relationship.

Contractual Safeguards: Include specific security requirements and incident response protocols in contracts to ensure accountability in the event of a breach.

Collaboration and Communication: Maintain open communication with third parties to quickly address new threats and ensure coordinated responses.

3. Harness AI and Automation

Artificial Intelligence (AI) and automation are powerful tools for enhancing exposure management. Implement these technologies to:

Automate Vulnerability Scanning: Use AI-powered tools for faster and more accurate identification of potential risks.

Utilize Predictive Analytics: Employ AI to predict potential cyberattacks, allowing proactive measures to protect assets.

Real-Time Monitoring: Deploy automated systems to continuously monitor networks, providing early detection of unusual activities.

Accelerate Incident Response: Leverage AI-driven tools to contain threats quickly, minimizing damage and reducing costs associated with breaches.

4. Implement Proactive Vulnerability Management

A proactive approach to vulnerability management is crucial for reducing overall exposure to threats. Businesses should:

Perform regular Scanning and Assessment: Conduct frequent vulnerability scans to identify and address potential weaknesses.

Prioritization: Focus remediation efforts on vulnerabilities that pose the greatest risk to critical business functions.

Patch Management: Keep systems and software up to date with the latest security patches.

Employee Training: Regularly train employees in cybersecurity best practices to reduce the risk of human error.

5. Prepare for the Unknown Unknowns

The most challenging risks are those that haven't been identified. To manage these "unknown unknowns":

Scenario Planning: Regularly conduct exercises to anticipate potential threats and develop appropriate responses.

Flexible Response Plans: Ensure response strategies are adaptable to new and unforeseen threats.

Continuous Learning: Stay informed about the latest cybersecurity trends and invest in ongoing education for your security teams.

Industry Collaboration: Share information with industry peers to identify and mitigate new threats more effectively.

Final Thoughts: Don't Let Exposure Get You Down

Exposure management is not a walk in the park,; but it doesn't have to be a nightmare either. With the right tools, resources, and strategies, you can navigate the challenges of this ever-evolving field. Remember, it's not about eliminating all risks because that's impossible, it's about understanding and managing them effectively. Whether you're deep in the trenches of cybersecurity or just starting out, keep calm and stay informed. And next time you're in a meeting discussing the latest vulnerabilities, remember; you're not alone. We're all trying to manage exposure in our own way, one whack-a-mole at a time.

CHOOSING BUSINESS PARTNERS:

BEWARE OF THE HIDDEN RISKS

BRIAN B. MUKALAZI
Finance & Strategy Expert
C. E. O, Talis Consults Ltd

Many years ago, somebody told me: "A person you do business with is more important than the business itself". And to this day, I consider these words to be the best business advice I have ever received.

Starting and running any business involves a large amount of risk. But many times, when we think of business risks, we tend to focus on cash flow issues, shifting market conditions or competition, and we pay less attention to the most important of them all - the risks associated with people or entities we do business with!

It doesn't really matter whether it's a start-up, an SME, a mature entity or a large-scale project. The simple fact is that those you choose to do business with are crucial and could make or break you.

Strategic business partnerships or relationships can take different forms, such as equity partnerships, financing partnerships, professional advisory partnerships, operational partnerships and distribution partnerships, among others. In this article, due to space limitations, we will delve into only the first three partnership forms.

Equity Partnerships (Involving Co-owners, Co-founders, etc.)

An equity partner invests capital and takes ownership in your business. While they can bring significant resources, an untrustworthy or incompatible partner can lead to financial loss or internal conflict. For example, imagine a small business owner who brings on an equity partner with substantial industry experience. The partner contributes financially, but as time goes on, it becomes clear that they have different values and ethical standards, leading to disputes. Worse, if the partner acts unethically, their actions could harm the company's reputation, affecting existing and future clients.

In October 2024, an article appeared in the Monitor Newspaper, reporting a gold scam story where an investor allegedly lost UGX 5 billion to fraudsters in Uganda. The article implicated a senior lawyer and partner at Shonubi, Musoke & Co. Advocates, a Kampala-based law firm. In a subsequent public notice, the firm vehemently denied any involvement in the scandal and noted that its partner's alleged actions were conducted without the firm's knowledge or authorization. The notice further revealed that the said partner had been asked to step down from the firm in order to attend to the matter.

While the firm should be commended for its decisive response, at that point, it could not undo the damage that had already been inflicted on its public image and reputation. For a firm of Shonubi, Musoke & Co's stature, such scandals could have dire consequences. And of course, it also remains debatable as to whether a firm can completely disassociate itself from its partners, let alone founding partners.

This scandal got me thinking: Did the firm previously conduct any periodic evaluations on its partners to review and assess their performance, commitment, reliability or ethical conduct? If yes, did it have any remedies for identified sub-par performance or results? These and similar questions remain unanswered.

In choosing (or maintaining) business partners, it's important that you always assess how well you fit with them. This means continually evaluating their vision, values, and reputation, as well as their capabilities and financial standing. A good fit is one that creates value for all parties, enhances competitive advantage, and supports the business's long-term vision.

For a business relationship to thrive, partners must demonstrate high levels of integrity and commitment, in order to build trust, which is the umbilical cord that keeps the business together. This would involve building and maintaining a positive and respectful relationship with each other, based on mutual understanding, transparent communication, and collaboration. But when things go awry, there should be clear exit plans!

> A person you do business with is more important than the business itself

Financing Partnerships (Involving Bankers, Lenders, Investors, etc.)

Financing partnerships typically refer to collaborative agreements, where financial institutions, such as banks and lenders, work together with investors or other capital providers to fund a business or project. Between 2012-2014, businessman Peter Kamya (now deceased), through his company Simbamanyo Estates Ltd, acquired loan facilities in excess of US $7.1 million from Equity Bank Uganda and its sister Bank in Kenya. The facilities were secured by mortgaging several properties, including Simbamanyo House (later renamed 'Gender and Labour House') located in the Kampala Central Business District, and the Afrique Suites Hotel in Mutungo, a Kampala suburb.

In 2021, after a protracted legal battle that also involved the intervention of the Ugandan President, the said properties were auctioned and sold by Equity Bank in an effort to recover an unpaid cumulative loan balance of more than US $10 million. On his part, the businessman pointed to several alleged illegalities in the loan process and argued that the foreclosure of his properties was marred with fraud. He accused the Bank of breach of trust and unethical behaviours.

The argument here is two-fold:

(1) For Equity Bank: What kind of risk assessment did the bank undertake before advancing the loans? Did the bank deploy any experts with the right industry knowledge and experience to review the client's business plans and advise on their viability? In my experience, loan performance is mostly decided at the assessment stage.

(2) For Simbamanyo Estates: What informed the decisions of obtaining the said loans? I have severally written about the risks associated with undisciplined business growth. Unfortunately, many companies have collapsed because of the undisciplined pursuit for growth, when much of it simply doesn't fit within their strategic insights and capabilities.

In addition, irrespective of the competitive loan terms, did the company ever conduct a compatibility check to determine whether the bank clearly understood its vision and unique challenges? A compatible financing partner is always more interested in your success and may provide tailored solutions to meet your specific business needs.

Professional Advisory Partnerships (Involving Accountants, Lawyers, etc.)

Professional advisory partnerships are arrangements where professionals from various fields—such as accountants, lawyers, and financial advisors—come together to provide specialized guidance and expertise to businesses, organizations, or individuals.

I am quite certain that many of our readers have heard about the Enron scandal that rocked the United States in the early 2000s. Before its demise, Enron was a large company based in Texas and its collapse affected over 20,000 employees. It was declared bankrupt on December 2, 2001. A major player in the Enron scandal was Enron's accounting firm, Arthur Andersen LLP, that was one of the Big 5 CPA firms globally.

Arthur Andersen, after having served as Enron's long-term auditor and consultant, was found guilty of several charges related to lack of professional behaviour and competence, including gross negligence of duty, fraud, non-application of appropriate accounting and auditing standards, and issuing incorrect audit reports.

There's a lot to consider when choosing a professional business advisor. Credentials, technical experience and affordability are all critical factors, but what I find to be even more critical is the ethical conduct and personality of the potential professional partner. If you're trusting a consultant or advisor with your business, then you want to make sure that they are of an upstanding moral character.

It is, therefore, important to thoroughly review their past track record and references as part of the decision-making process. By obtaining feedback from previous clients, you can gain valuable insights into their performance, reputation, and ability to achieve desired results. Also, it is a good practice to periodically change these advisors to mitigate risks associated with long-term advisor-client relationships. And make no mistake, even large professional firms can make costly blunders.

In Conclusion

The complex nature of businesses everywhere, inherently gives rise to risk. But by choosing the right business partners in the first place, you can reduce that risk tremendously.

Finally, do not be afraid to re-evaluate a failed partnership. A business partnership that failed in the past might work in the future. Business environments change. People change. And it is, therefore, a mistake to just write off any relationship as a lost cause.

DEVELOPING AN EFFECTIVE RISK MANAGEMENT STRATEGY

JESSE OKUTRE
Operational Risk Specialist, NSSF

Having a robust risk strategy is critical for any organization aiming to navigate the complexities of today's business environment. A well-developed risk strategy helps identify, assess, and mitigate potential threats that could disrupt operations, ensuring business continuity and stability.

By proactively managing risks, organizations can protect their reputation, minimize financial losses, and enhance decision-making processes. Moreover, a good risk strategy fosters innovation and growth by providing a secure framework within which new ideas can be explored without jeopardizing the organization's core objectives.

In essence, an effective risk management strategy is not just about avoiding pitfalls but also about seizing opportunities in a controlled and informed manner.

Before I delve into the details of developing an effective risk management strategy, let me highlight some of the advantages of having a good risk management strategy.

i) Reduced risk exposure

Effectively managing risks safeguards an organization's physical security, data, information security and reputation. By identifying and addressing vulnerabilities and implementing controls, companies can enhance their security posture and reduce the likelihood and impact of potential threats.

ii) Enhanced resilience

Effective risk management strategies allow organizations to identify potential risks proactively. By continuously monitoring and assessing business environment, organizations can take proactive measures to prevent, mitigate, or eliminate the risks before they materialize. This proactive approach helps avoid costly disruptions, errors, and operational failures.

iii) Improved organizational performance

Effective risk management strategy shields your organization from financial losses, fines, penalties, and reputational harm due to risk events. By implementing suitable controls and mitigants, you can reduce the frequency and severity of these events, ensuring financial stability and protection of your company's reputation and improved organizational performance.

iv) Improved regulatory compliance

An effective risk management strategy can enhance regulatory compliance by proactively identifying and analyzing regulatory and contractual requirements, assessing the organization compliance status in respect of the regulatory and contractual obligations, and putting in place measures to prevent and detect non-compliance.

Integrated risk management improves compliance, risk identification, assessment and reporting across the organization. This integrated approach ensures that compliance considerations are integrated into decision-making processes, supported by robust documentation and tracking mechanisms. Consequently, organizations can better adhere to regulatory standards, avoid legal penalties, and maintain a strong reputation.

V) Increases the organization's competitive edge

A good risk strategy enhances organizational competitiveness by providing a holistic framework for managing risks across the organization. It ensures that potential threats are managed before they escalate, thereby minimizing disruptions and financial losses. Additionally, enterprise risk management (ERM) aligns risk management with strategic planning, enabling better decision-making and resource allocation. By fostering resilience and agility, ERM helps organizations capitalize on opportunities, maintain operational continuity, and protect their reputation, ultimately leading to sustained competitive advantage.

Having highlighted the advantages of an effective risk management framework, the next question that comes to

mind is, how do you develop an effective risk management strategy?

a) Alignment of risk strategy with organization strategy.

The ultimate objective of risk management is to enable the organization to attain its objectives, because risk affects the objectives. ISO 31000- Risk Management, defines risk as "the effect of uncertainty on an objective, whether positive or negative".

Understanding organizational objectives is critical when developing a risk strategy. These objectives provide a clear direction and framework for identifying, assessing, and managing risks that could impact the organization's ability to achieve its objectives.

By aligning the risk strategy with the organization's overall goals and strategic priorities, risk management efforts become more focused and effective. This alignment ensures that risk management activities support the organization's mission and vision, promoting a strong risk culture and enhancing decision-making processes.

b) Continuous risk assessment

Risk identification and assessment are foundational steps in developing an effective risk strategy. This process involves systematically identifying potential risks that could impact the organization's objectives, using various methods such as workshops, interviews, surveys, and data analysis.

Once identified, these risks are assessed based on their likelihood and potential impact on the organization, this allows the organization to prioritize identified risks. The process of prioritizing helps in allocating resources efficiently and developing targeted risk mitigation strategies, thus enhancing organization reliance through making informed decisions and making better preparations for uncertainties.

c) Define risk appetite and risk tolerance

Clearly define and communicate risk appetite and risk tolerance limits to all relevant stakeholders. Risk appetite defines the amount and type of risk an organization is willing to pursue or retain to achieve its objectives, while risk tolerance specifies the acceptable levels of variation in performance related to these risks. Risk appetite and risk tolerance limits define psychological boundaries of decision-making.

Understanding and applying these concepts helps organizations to make informed decisions about which risks to accept, mitigate, or avoid. These concepts ensure that risk-taking aligns with the organization's strategic goals and capacity to manage potential adverse outcomes.

Clearly defined risk appetite and tolerance levels also facilitate consistent risk communication across the organization, fostering a unified approach to risk management.

During the process of developing a risk strategy, risk response strategies provide a structured approach to addressing identified risks. These strategies include risk avoidance, reduction, transfer or acceptance, each designed to address the nature and severity of the risk. By implementing appropriate risk response strategies, organizations can mitigate potential negative impacts, capitalize on opportunities, and ensure continuity of operations. Effective risk response augments decision-making by providing clear actions and contingency plans, thereby reducing uncertainty and increasing organizational resilience.

d) Risk monitoring and reporting

Continuous monitoring ensures that risk management processes remain dynamic and responsive to changing operational conditions and environments, allowing organizations to detect emerging risks early and adjust their strategies accordingly.

Regular risk reporting provides transparency and accountability, enabling stakeholders to stay informed about the risk landscape and the effectiveness of risk management efforts. This ongoing oversight helps in maintaining alignment with organizational objectives and regulatory requirements. Additionally, monitoring and reporting facilitate a culture of continuous improvement, where lessons learned from incidences and past experiences are integrated into future risk management practices.

e) Stakeholder engagement

It is usually important to get the perspectives and concerns of all relevant stakeholders in developing a risk management strategy. By involving stakeholders such as employees, customers, suppliers, and regulators, organizations can gain a comprehensive understanding of the risks they face and the potential impacts on various aspects of the business. This inclusive approach helps in identifying and prioritizing risks more effectively, as stakeholders often provide insights that might not be apparent to the risk management advisory team alone. Additionally, engaging stakeholders fosters a sense of ownership and commitment to the ERM process, enhancing the overall risk culture within the organization.

f) Scenario planning and stress testing

Scenario planning and stress testing are vital tools in risk management. These tools allow organizations to anticipate and prepare for potential adverse events, by simulating various scenarios and assessing their impacts on the business.

Scenario planning helps identify and evaluate the effects of different risk factors, enabling organizations to develop strategies to mitigate these risks proactively. Stress testing, on the other hand, evaluates the resilience of the organization under extreme conditions, assessing whether it can withstand significant shocks and continue to operate effectively.

By incorporating these techniques, organizations can better understand the interconnections between different risks and their potential cumulative effects. This comprehensive approach not only enhances risk awareness but also supports more informed decision-making and strategic planning, ultimately leading to a more robust and resilient ERM strategy.

In Conclusion

Effective communication and collaboration with top management and other stakeholders helps facilitate the implementation of risk management strategies, ensuring that they are practical and are aligned with the organization's objectives, to ensure long-term success, resilience and stability in times of uncertainty. Additionally, effective risk management strategies, if well-aligned to the organization's strategic objectives, help allocate resources effectively by focusing on the most critical risk.

THE CYBER Mamushka

CYBER SAFETY THAT PROTECTS

what matters most—your family.

Cyber safety begins at home! Just like locking your doors keeps intruders out, protecting your digital life is just as important.

- Practical, everyday cybersecurity for families.
- Simple, easy-to-follow steps—no tech skills needed!

OUR SERVICES & PRODUCTS

- **Cyber Safety Awareness** - *Weekly articles to help you stay safe online*
- **Courses & Quizzes** - *Learn & test your cyber skills*
- **CyberSafe or CyberSorry? Card Game** - *Play. Learn. Stay CyberSafe*
- **Checklists & Guides** - *Quick safety tools*
- **Incident Response Advisory** - *Help when cyber threats strike*

CONTACT US

www.thecybermamushka.com

paulinekire@thecybermamushka.com

0701550243

OFFICE

Kampala Road, Butabika

THE PSYCHOLOGY OF PHISHING: WHY WE CLICK AND HOW TO STOP

PAULINE KIRE

Offensive Security Tester,
Stanbic Bank Uganda

It happens in an instant: a carefully crafted email lands in your inbox, disguised as an urgent message from your bank, a colleague, or even your favourite online store. It looks legitimate - professional logos, convincing language, and just enough personal detail to make you pause. You click the link without a second thought. And just like that, the cybercriminals have won!

Have you experienced this scenario before? Tap your chest three times and say, "I need to do better."

This scenario plays out daily across the globe, costing organizations and individuals billions of dollars each year. Phishing remains one of the most effective tools in a cybercriminal's arsenal, not because of technical brilliance but because it preys on the psychology of human behaviour. Understanding why we fall for phishing attacks and how to stop them, is key to reducing this pervasive threat.

Why Do We Fall Prey To Phishing?

Cybercriminals are masters of psychological manipulation, exploiting common human tendencies and emotions. Let's dive into the "why" behind the clicks - don't worry, this isn't therapy, but it might feel like it.

i) We are wired for Trust: Humans are naturally inclined to trust others - it's how we've survived and thrived as a species. Cybercriminals exploit this trust by impersonating familiar brands, colleagues, or authority figures. A phishing email from "HR" about an urgent payroll issue taps into that trust and compels immediate action.

ii) We respond to Urgency: Phishing emails often use time-sensitive language: "Your account will be locked in 24 hours," or "Action required immediately!" This sense of urgency overrides our ability to think critically, prompting us to act before we analyse the situation.

iii) Fear of Missing Out (FOMO): Phishing scams often appeal to our fear of loss - whether it's a missed package delivery, a compromised bank account, or a lost job opportunity. These emotional triggers make us more likely to take the bait.

iv) Authority: Cybercriminals often impersonate figures of authority, such as company executives, law enforcement, or government officials. This tactic leverages the psychological pressure to comply with authority figures, making individuals feel obligated to act.

v) Reciprocity: By offering something of perceived value such as a free gift, discount, or insider information; cybercriminals create a sense of obligation. Victims feel compelled to "return the favour" by clicking a link or providing information.

vi) Social Proof: Phishers use testimonials, endorsements, or references to others' actions to persuade victims. For example, an email might claim, "Over 1,000 people have already signed up!" People are naturally inclined to follow the crowd, especially when uncertain.

vii) Scarcity: Limited time offers or exclusive opportunities, such as "Only 5 spots left!" or "Claim your prize before midnight!" are designed to create a sense of scarcity. This triggers impulsive decision-making, bypassing rational thought.

How to Avoid Falling A Victim

While phishing is a common challenge, it is solvable. Here's how you can stop falling victim to these clever attacks:

a) Pause Before You Click: Train yourself to pause and evaluate every unexpected email, especially those requesting sensitive information or immediate action. A moment of caution can prevent a costly mistake.

b) Verify Every Request: Even the most convincing emails can be fake. Cybercriminals often impersonate trusted entities or people to get you to act. Check the sender's email address carefully. Cybercriminals often use addresses that are similar to legitimate ones but with subtle differences (e.g., support@paypall.com instead of support@paypal.com). Use a separate, trusted channel to confirm (e.g., call your bank directly using the number on their website).

A carefully crafted email lands in your inbox, disguised as an urgent message from your bank, a colleague, or even your favourite online store.

It looks legitimate

c) Look for Red Flags: Phishing emails often include small but telling errors, such as:

- Generic greetings like "Dear Customer" instead of your name.
- Grammatical mistakes or awkward phrasing
- Links that don't match the official website (hover over links to preview their destination).

d) Leverage Technology: Organizations and individuals should use tools like:

- Email filtering systems to block suspicious messages.
- Multi-factor authentication (MFA) to add an extra layer of security.
- Antivirus software to detect and quarantine malicious files.

e) Educate Yourself and Others: Ongoing education is critical to staying ahead of phishing tactics. Participate in phishing simulations, attend cybersecurity training, and share your knowledge with family and colleagues.

The role of organization in phishing prevention.

While individual vigilance is essential, organizations play a crucial role in creating a security-first culture through:

i) Phishing Simulations: Regularly conduct simulated phishing attacks to test and train employees. These exercises help identify vulnerabilities and reinforce best practices.

ii) Open Communication: Encourage employees to report suspicious emails without fear of judgment. A "no-blame" culture ensures that potential threats are addressed quickly.

iii) Clear Policies: Provide employees with clear guidelines for handling sensitive information, verifying requests, and escalating concerns.

iv) Turning Awareness Into Action

By prioritizing education and fostering a supportive environment, organizations can significantly reduce their exposure to phishing attacks. Phishing isn't going away anytime soon, but neither is our ability to outsmart it. The key lies in recognizing that cybersecurity is as much about people as it is about technology. By understanding the psychological tactics cybercriminals use and empowering ourselves with knowledge and tools, we can turn the tide against phishing.

So, next time you receive an urgent email demanding your immediate attention, take a moment to pause, think, and verify. After all, cybersecurity starts with you and sometimes, the best defense is simply not clicking.

In Conclusion

Phishing may prey on our trust, urgency, and fear, but education and vigilance can dismantle its effectiveness. Whether you're an individual managing your personal inbox or a leader responsible for organizational security, understanding the psychology of phishing is the first step to building a stronger and safer digital future.

THE ROLE OF HUMAN BEHAVIOUR IN RISK MANAGEMENT

JOSHUA KIBIRIGE
Operational Risk & Anti-Money Laundering Manager, NSSF

Risk management is the discipline of identifying, assessing, and mitigating risks to ensure the stability and success of an organization. An essential part of this process is maintaining a balance between taking risks that offer opportunities for growth and managing threats that could lead to failure.

Human behaviour plays a pivotal role in the success or failure of risk management strategies, as it directly influences how individuals and organizations perceive, assess, and respond to potential threats.

For instance, aggressive human behaviour can lead to risky investments, while a fear of loss may cause individuals or organizations to avoid necessary risks, resulting in missed opportunities.

This article examines the role of human behaviour in achieving effective risk management.

Aggressive behaviour

One critical aspect of human behaviour that can significantly impact risk management is aggressive behaviour. While it may drive quick decisions and rapid action, aggressive behaviour often leads to excessive risk-taking, bypassing established controls, and overlooking potential threats.

Aggressive behaviour played a significant role in causing the 2008 financial crisis, primarily through excessive risk-taking, reckless decision-making, and disregard for caution in both the financial sector and broader economic environment. Leading up to the crisis, major financial institutions like banks, mortgage lenders, and investment firms aggressively pursued high-risk strategies to maximize short-term profits. Many financial players adopted highly speculative practices, such as:

1. Subprime Lending:

Banks and mortgage lenders aggressively extended loans to individuals with poor credit history (subprime borrowers). This risky lending practice was driven by the desire to generate more business and capitalize on rising home prices. Financial institutions disregarded assessment of borrowers' ability to repay loans, assuming that housing prices would continue to rise indefinitely.

2. Securitization and Mortgage-Backed Securities (MBS):

Aggressive behaviour led to what is known as securitization, which involved packaging of risky subprime loans into complex financial products, such as mortgage-backed securities and collateralized debt obligations (CDOs). Banks and financial institutions aggressively pushed these products onto investors, often downplaying or misrepresenting the risks involved. These securities were marketed as safe investments, even though they were based on high-risk loans.

Financial institutions became increasingly aggressive in leveraging, meaning they borrowed substantial amounts of money to invest in risky assets. This amplified potential gains but also greatly increased the risk of catastrophic losses if asset values fell. Several key behaviours emerged during this time:

3. Weak Risk Management:

Aggressive financial behaviour often bypassed traditional risk controls. Many institutions ignored warning signs, failed to adequately assess risk, and pursued profits without implementing strong checks and balances. Risk management was viewed as a barrier to profit, leading to a culture where proper risk mitigation was downplayed or ignored.

Aggressive lending behaviour also manifested in the real estate market, with both individuals and institutions speculating on the continuous rise in housing prices. Mortgage lenders aggressively pursued borrowers, offering "teaser rates" or "no documentation" loans that allowed people to borrow more than they could afford.

These loans were marketed to individuals with low income or poor credit scores, contributing to the eventual spike in loan defaults when housing prices fell.

While aggressive behaviour may be driven by a desire for rapid growth or success, it can jeopardize the core

principles of effective risk management, which emphasize careful assessment and mitigation.

Effective risk management relies on sound governance structures, where decisions undergo appropriate levels of review and scrutiny. Aggressive behaviour, especially from leadership, can erode this governance practice. When individuals or teams push through risky initiatives without following established procedures or bypass key decision-makers, it undermines the checks and balances needed for effective risk control. Over time, this leads to a breakdown in accountability, making it easier for reckless or unvetted risks to be taken. When risk governance is compromised, the entire organization becomes vulnerable to cascading failures.

Aggressive behaviour often introduces bias into the risk assessment process, leading to overly optimistic projections or the downplaying of potential hazards. For example, an organization might overestimate its ability to enter a new market quickly, while underestimating the regulatory or competition risks involved.

When risk management is compromised, companies may take on excessive risks without having the necessary contingency plans in place, leaving them exposed to severe consequences. Understanding the influence of aggressive behaviour is essential for ensuring that risk management remains effective and balanced.

Risk-averse behaviour

On the other hand, the risk averse behaviour can distort decision-making in risk management by leading to overly cautious behaviour. When individuals or organizations are excessively focused on avoiding losses, they may prioritize short-term safety over long-term growth. This creates a conservative approach of desiring to maintain the status quo rather than pursuing potentially rewarding opportunities. While this may reduce immediate risks, it can also hinder the organization's ability to adapt to changes or capitalize on opportunities in dynamic markets.

For example, the fear of taking risks played a critical role in Nokia's decline from its position as a global leader in the mobile phone industry. While Nokia was once the dominant player in the mobile market, its reluctance to embrace emerging technologies and take bold strategic risks allowed competitors, particularly Apple and Google (Android), to overtake the company.

As Apple and Android aggressively pursued app ecosystems with their App Store and Google Play, Nokia was slow to adapt. It underestimated the value of third-party apps and the power they had to attract users. Nokia's fear of fully committing to the app-driven model left it with fewer opportunities to compete in the rapidly evolving smartphone landscape.

Nokia's corporate culture during the period leading up to its decline became increasingly risk averse. The company's leadership, particularly in its top management, feared the potential fallout from making radical changes to its strategy or products.

In Conclusion,

For effective risk management, organizations need to strike a balance between these two extreme behaviours by taking calculated risks and ensuring that these risks are managed appropriately in order to achieve long-term success and sustainability.

Ultimately, organizations that embrace a balanced approach to risk management that allows for both aggressiveness and cautiousness will be better positioned to navigate an increasingly complex and competitive business environment. By doing so, they can safeguard their operations while continuing to grow and evolve.

WASTE MANAGEMENT: A GLOBAL CONCERN

CHARLES KATENZA
Audit and Compliance manager,
Multi-Community Based Development Initiative.

In the modern era, waste management has become one of the most pressing environmental challenges facing the world. With the global population soaring, currently over 8.1 billion people (https://www.worldometers.info/world-population/), and consumption patterns intensifying, with urban population estimated to be 4.4 billion, the volume of waste generated is increasing at an unprecedented rate.

Effective waste management is not just an environmental issue—it is a public health obligation, an economic necessity, and a crucial aspect of sustainable development.

The Growing Challenge of Waste

According to the 2024 Global Waste Management Outlook by UNEP, urban solid waste generation is expected to rise from 2.1 billion tonnes in 2023 to 3.8 billion tonnes by 2050. The report predicts that waste management costs will nearly double within a generation, and that only a significant reduction in waste generation can ensure a sustainable future.

Therefore, when the world generates over 2 billion tonnes of solid waste each year, and this figure being projected to rise significantly in the coming decades, actions need to be taken now!

Coupled with the increasing volume of waste globally, the nature of waste has also changed, with more complex materials, such as electronic waste (e-waste), plastics, and hazardous substances, making waste management increasingly difficult. Urbanization and industrialization are major contributors to this growing challenge. Cities in particular, face significant waste management challenges due to their dense populations and high levels of consumption. Rapid urban growth in developing countries has outpaced the development of adequate waste management infrastructure, leading to severe environmental and health issues.

The Environmental Impact of Poor Waste Management

Inefficient or inadequate waste management has far-reaching environmental consequences. One of the most visible impacts is the pollution of land, water, and air. Landfills, often the primary method of waste disposal, can release harmful chemicals into the soil and groundwater, leading to contamination. Methane, a potent greenhouse gas, is also emitted from landfills, contributing to climate change.

Marine pollution is another critical issue. Each year, millions of tonnes of plastic waste enter water bodies, harming marine life and disrupting ecosystems. Microplastics, which result from the breakdown of larger plastic items, have been found in the food chain, raising concerns about human health impacts.

In addition to pollution, poor waste management practices can lead to the loss of valuable resources. Materials that could be recycled or repurposed often end up in landfills, wasting resources that could otherwise be reintroduced into the production cycle.

Public Health Implications

The consequences of waste management are far-reaching, which include loss of lives. According to new vision of August 10th, 2024, Uganda was hit with a disaster of a landfill in Kiteezi, in Kampala metropolitan area, that was caused by a garbage sludge, where over 35 people were reported to have died.

The mismanagement of waste also poses significant public health risks. Inappropriate waste disposal can lead to the proliferation of disease vectors, such as rats and mosquitoes, which thrive in unsanitary conditions. In many developing countries, informal waste workers who often lack protective equipment, are exposed to hazardous substances, leading to serious health problems.

The burning of waste, a common practice in areas without proper waste management infrastructure, releases toxic fumes that contribute to respiratory diseases and other health issues. Communities living near landfills or waste treatment facilities are often disproportionately affected by these health risks, highlighting the environmental implications of inappropriate waste management.

Economic Costs of Waste Mismanagement

The economic costs of poor waste management are substantial. Inefficient waste systems can strain public budgets, especially in developing countries, where resources are already limited. The costs associated with cleaning up pollution, addressing public health crises, and managing landfills, can be significant.

On the other hand, effective waste management presents

economic opportunities. Recycling and waste-to-energy programs can create jobs and generate revenue. The publication by Bruna Alves in January 2024, indicated that the global waste recycling services market was valued at an estimated US $58 billion in 2022. The market is expected to grow considerably in the coming years as consumer awareness about the environmental impacts of waste increases. By 2032, the global waste recycling services market is forecasted to have surpassed a value of US $90 billion, registering a compound annual growth rate (CAGR) of 4.7 percent during the forecast period 2023 to 2032. This, therefore, offers significant economic potentials for countries and entrepreneurs altogether to be able to invest in this sector that should not be ignored.

The Path Forward: Sustainable Waste Management Solutions

Addressing the global waste crisis requires a multifaceted approach that includes reducing waste generation, improving waste collection and disposal, and promoting recycling and resource recovery.

1. Waste Reduction at the Source

Reducing waste begins with changes in production and consumption patterns. Manufacturers can play a key role by designing products that generate less waste, are easier to recycle, and have longer life spans. Consumers, too, can contribute by adopting more sustainable lifestyles, such as reducing single-use plastics and choosing products with minimal packaging.

2. Improved Waste Collection and Disposal

Effective waste collection and disposal systems are essential for managing waste sustainably. This includes the development of adequate infrastructure, particularly in rapidly urbanizing areas. Governments need to invest in modern waste management facilities and technologies that minimize environmental impacts, such as sanitary landfills, composting facilities, and waste-to-energy plants.

3. Promotion of Recycling and Resource Recovery

Recycling is a critical component of sustainable waste management. Governments and businesses must work together to develop recycling programs that are economically viable and accessible to all communities. Public education campaigns can help increase awareness and participation in recycling programs.

4. Innovation in Waste Management Technologies

Technological innovations offer promising solutions to the waste management challenge. Advances in waste sorting, treatment, and recycling technologies can improve the efficiency of waste management systems. Waste-to-energy technologies, which convert waste into usable energy, can also play a significant role in reducing the volume of waste that ends up in landfills.

5. Global Cooperation and Policy Frameworks

Waste management is a global issue that requires international cooperation. The development of global policy frameworks, such as the Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and thier Disposal, is crucial for managing waste across borders. Countries must work together to share best practices, technologies, and resources to tackle this global challenge.

In conclusion, therefore, waste management is a global concern that requires urgent and sustained action from governments, businesses, and individuals alike. The environmental, public health, and economic implications of poor waste management are too significant to ignore. By adopting sustainable waste management practices, investing in innovative technologies, and fostering international cooperation, we can turn the waste challenge into an opportunity for creating a cleaner, healthier, and more sustainable world for future generations.

POLITENESS AND RUDENESS:

THEIR IMPACT ON ORGANIZATION PERFORMANCE.

MICHEAL SENDIWALA

Senior Investment Risk Manager, NSSF

In the realm of organizational behaviour, the dynamics of interpersonal communication play a crucial role in shaping workplace culture and overall performance. Politeness and rudeness are two contrasting communication styles that significantly influence employee engagement, collaboration, and productivity. Understanding their impact can provide valuable insights for leaders and organizations aiming to foster a positive work environment.

Politeness is the practice of being considerate and respectful towards others in communication and social interactions. Politeness is a soft but powerful communication tool that can calm tempers, enlist sympathy and favours, and most importantly politeness can help to resolve conflicts. On the contrary, rudeness is a catalyst for conflicts; rudeness is a type of behaviour that is inconsiderate, insensitive, deliberately offensive, impolite, obscene, or that violates society norms.

In African tradition, children were expected and indeed they exercised politeness before their parents and other elders, women exercised politeness before men, servants exercised politeness before their masters, etc. Children, women, and servants who were rude to their parents and other elders, men and servants respectively, were reprimanded to say the least. As a result, families and communities lived in harmony.

However, it is interesting to note that in the contemporary world, particularly in the capitalist West, politeness is regarded as naivety, meekness and lack of self-esteem and confidence. Nonetheless, politeness can have profound positive impact on employee engagement, while a rude culture creates toxic work environment.

It is, therefore, important to nature a polite culture as explained below:

Enhanced team collaboration

Politeness encourages open dialogue and teamwork. If leaders are polite in their communication and social interactions, employees are likely to share ideas and provide constructive feedback to their leaders, which helps to create improvements in many areas, including but not limited to strategy, processes, systems and products.

Increased job satisfaction

If employees feel respected and valued, their morale will most certainly be high, and they will enjoy what they do; and in the process their productivity will increase. Consequently, there will be low staff turnover and reduced recruitment costs.

Better conflict resolution

When employees approach disagreements with respect, they are more likely to find a common ground and resolve issues amicably. Courteous interactions can mitigate conflicts before they escalate.

Positive organization culture

This, not only attracts a wider range of talent, but also enhances the organization's reputation, making it an employer of choice. A culture that prioritizes politeness promotes inclusivity and diversity, its tonality scores are likely to be high.

Conversely, rudeness can have far reaching negative consequences for an organization, as a case for Uber. In 2017, Uber served as a compelling example of how a rude and toxic culture can lead to significant challenges for a company, including high turnover and reputational damage.

At that time, the company was led by co-founder and former CEO Travis Kalanick, whose aggressive management style set a tone for the organization. Reports indicated that Kalanick often exhibited rudeness and a lack of respect for employees, leading to a culture that tolerated abrasive behaviour.

Employees described it as a high-pressure environment where aggressive tactics were not only accepted but encouraged. This led to a culture of fear and competition, where team members often undermined each other to get ahead.

As highlighted in the case above, rudeness results into;

a) Decreased employee engagement

Rude behaviour can create a toxic atmosphere where employees feel undervalued and demotivated. This disengagement can lead to decreased productivity and a lack of initiative.

b) Increased stress and anxiety

A culture of rudeness often results in heightened stress levels among employees. This can lead to burnout, absenteeism, and ultimately, a decline in performance.

c) Poor team dynamics

When employees experience or witness lack of courtesy, driven by rude behaviours, it can lead to mistrust and a breakdown in communication, hindering collaboration and effectiveness. Rudeness disrupts team cohesion.

d) Damage to reputation

Organizations known for a rude culture can suffer reputational damage, making it difficult to attract and retain top talent. This can have long term negative effects on growth and success of the organization.

To harness the benefits of politeness and mitigate the effects of rudeness, organizations can implement several strategies, including but not limited to the following:

Lead by example

Leadership plays a pivotal role in setting the tone for workplace behaviour. Leaders who model polite and respectful communication, establish a standard for employees to follow.

Training and development

Providing training on communication skills, emotional intelligence, and conflict resolution can equip employees with the tools to engage in polite interactions.

Encourage feedback

Create channels for employees to provide feedback on workplace culture. This can help identify areas for improvement and reinforce the importance of respectful communication.

Recognize and reward politeness

Acknowledging and rewarding polite behaviour can reinforce a culture of respect. This could be through formal recognition programs or informal praises.

Address rudeness promptly

It's essential to address instances of rudeness swiftly and constructively. Ignoring negative behaviour can signal that it is acceptable, perpetuating a toxic culture.

However, as leaders are implementing the above measures, they must be cognizant of the unintended side effects, which politeness can have on organization performance. Below are some of the potential downsides to consider;

- A strong emphasis on politeness may lead employees to avoid giving direct feedback or addressing difficult issues. This, can result in unresolved conflicts or performance problems, ultimately hindering productivity and team cohesion.

Politeness and rudeness are two contrasting communication styles that significantly influence employee engagement, collaboration, and productivity.

- Excessive politeness may lead to superficial interactions, where employees prioritize being agreeable over authentic communication which can create a lack of trust and openness, preventing deeper collaboration and innovation.
- In an effort to maintain a polite atmosphere, employees may hesitate to challenge ideas or propose alternatives. This can slow down decision-making processes and lead to suboptimal choices, as dissenting voices may not be heard.
- Employees may feel frustrated if they perceive politeness as insincerity or a facade, leading to resentment, which can damage morale and foster a culture where employees are disengaged or less motivated.
- A polite culture may inadvertently shield individuals from accountability, as employees may hesitate to call out mistakes or shortcomings, which can lead to a lack of accountability and poorer overall performance.
- Employees might prioritize politeness over addressing underlying issues, resulting in a culture of avoidance.

  While short-term tensions may be minimized, long term conflicts can escalate and create a more challenging environment.

Organizations should encourage a culture that values both politeness and open dialogue, ensuring that employees feel safe addressing issues and providing honest feedback.

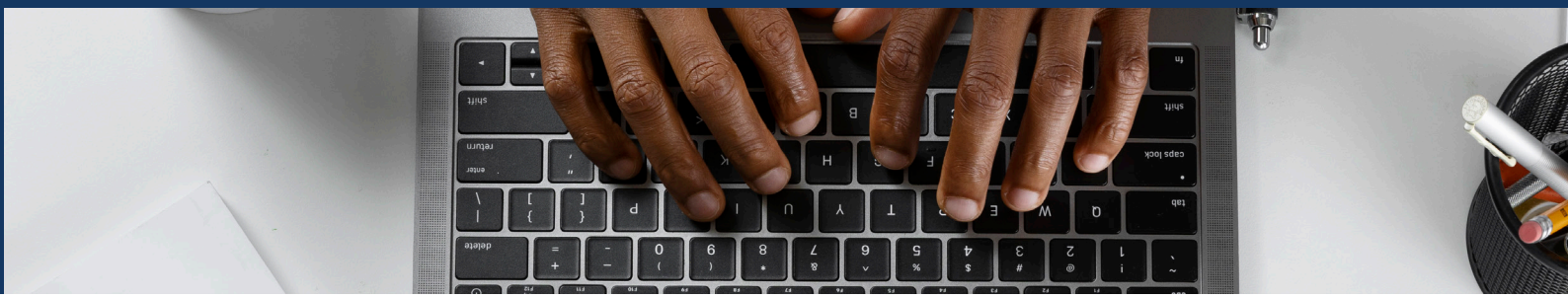
Conclusion

The impact of politeness and rudeness on organizational performance cannot be over emphasized. While politeness fosters a culture of respect, collaboration and innovation, rudeness can lead to disengagement, conflict, and decreased productivity. By prioritizing polite communication and addressing rudeness proactively, organizations can create a thriving workplace that enhances overall performance and well-being. However, it's essential to balance politeness with authenticity and direct communication.

THE DARK WEB:

"A HIDDEN WORLD OF OPPORTUNITIES AND THREATS"

NORBERT NAMANYA
Information Security Specialist, NSSF



The dark web, often associated with illicit activities and criminal enterprises, is a hidden part of the internet that operates outside the reach of ordinary internet search engines that ordinary internet surfers use like Google, Bing, MSN, Yahoo etc. It offers anonymity to its users by using specialized encryption tools such as Tor, to mask identities and locations. While often viewed as a dangerous digital underworld, the dark web is not purely a haven for illegal activities. In reality, it's a double-edged sword, a place where privacy and freedom can thrive but also where crime and exploitation are rampant.

The dark web can be broadly categorized into three types

1. Surface web overlay. This refers to sites accessible through regular browsers but require encryption tools, like Tor, for privacy, allowing users to navigate anonymously without search engines indexing them.

2. The deep web-accessible. This dark web comprises databases and hidden information behind private networks that hold subscription-based content and are accessible only to those with specific permissions or login credentials. Unlike content on the ordinary internet, these resources are "hidden" because they require users to know where to look and have a way to authenticate access, ensuring their privacy and exclusivity. This segment of the dark web can include sensitive information, like medical records, business confidential data, personal records, social security numbers, credit card numbers, etc., making it valuable.

3. Darknet-specific sites. This is exclusive to certain dark web networks like Tor, encrypted communities and marketplaces, where individuals interact in restricted forums for privacy-focused discussions or to access marketplaces not available on ordinary networks. Each type serves a different privacy and access level, catering for various user needs from privacy to controlled information exchange.

As we've seen, the dark web can be viewed as a necessary evil. Let's explore both sides of the dark web; the good and the bad, but most importantly understand how both organizations and individuals can benefit from the dark web, while protecting themselves against its dangers, particularly regarding data breaches, privacy preservation, and cyber threats.

The Good: The Bright Side of the Dark Web

Though often demonized, the dark web offers a crucial platform for those in need of secure communication. For individuals living under oppressive regimes where internet access is rationed by blocking sites that enable mass communication for information disseminations, the dark web provides a lifeline to the outside world.

Journalists, political protestors, and activists can communicate anonymously without fear of persecution. By using encrypted networks, whistleblowers can expose corrupt individuals, corporate malpractice, or human rights violations without revealing their identities.

There are also legal uses of the dark web. Researchers and academicians use it to discuss controversial topics in forums without the pressure of public scrutiny. Companies and security experts monitor the dark web for cyber threats to their organizations. In essence, the dark web can serve as a tool for those who require privacy and protection from external threats.

The Bad: Criminal Activity In the Dark Web

However, despite its potential for good, the dark web is notorious for harboring a roaring ecosystem of illicit activities. Illegal marketplaces offer everything from drugs and weapons to counterfeit documents and stolen data. One of the most infamous examples is Equifax data breach, one of US Credit Bureaus, had their data stolen in 2017 for approximately 145 million clients. Some of the stolen data included names, social security numbers, birth dates, addresses, phone numbers and driver's license numbers. This is personally identifiable information (PII) whose protection and privacy should be held in high regard by every organisation that is involved in collecting, storing and processing of personal information.

Cybercrime is rampant on the dark web. Hackers sell stolen sensitive data, leading to identity theft and financial loss for individuals and organizations. Ransomware and malware are traded openly in dark web forums, making it easier for criminals to launch cyber-attacks on unsuspecting targets. Human trafficking, exploitation, and child pornography are also horrific realities that continue to plague certain corners of the dark web, perpetuating its reputation as a dangerous digital space. While the anonymity provided by the dark web can protect vulnerable users, it also empowers criminals to act with impunity, making it a high-risk zone for anyone who ventures in it unprepared.

Impact of Stolen Data

The impact of stolen data on organizations, particularly in Uganda, can be severe, especially in light of the Data Protection and Privacy Act of 2019. This legislation mandates stringent measures for data handling, requiring organizations to implement robust security protocols to protect personal information, and providing for a penalty of 2% of gross turnover for any organization found guilty of data breach.

When a data breach occurs, organizations not only face the immediate ramifications of lost customer trust, damaged reputation and potential legal liabilities, but they also risk significant fines imposed by regulatory bodies for non-compliance with the law. As such, the consequences of stolen data go beyond immediate financial losses; they can undermine consumer confidence and lead to long-term operational challenges for organizations striving to align with data protection standards in an evolving regulatory landscape.

Protection: Staying Safe from the Dangers of the Dark Web

Given the potential risks, it's important for both individuals and organizations to take proactive steps to protect themselves from the dangers lingering on the dark web.

1. Dark Web Monitoring Tools.

Organizations can leverage specialized monitoring tools such as DarkOwl, Recorded Future, and CybelAngel to scan dark web sites for stolen data or mentions of their brand. These tools provide real-time alerts when sensitive information, such as login credentials or proprietary data, is discovered on the dark web. Regular monitoring helps organizations respond quickly to breaches and limit damage.

2. Engage with Threat Intelligence Services.

Partnering with cybersecurity firms that specialize in dark web threat intelligence is another effective strategy. Their services offer deeper insights into dark web activities, providing early warnings of potential data leaks, cyber-attacks, and threats to organization's reputation.

3. Monitor Employee and Customer Credentials.

Organizations should routinely monitor the dark web for leaked employee or customer credentials using services like "Have I Been Pwned" or "SpyCloud". These platforms alert users when their email addresses or passwords have been compromised in data breaches, allowing for quick action such as password resets or enhanced security measures.

4. Set Up Automated Alerts for Key Data.

Automated alert systems can notify organizations if specific keywords—such as the company's name, product names, or proprietary information—appear on dark web forums. These alerts provide early warnings about potential breaches, giving security teams time to address the vulnerabilities.

5. Search Dark Web Forums and Marketplaces.

For advanced cybersecurity teams, searching dark web forums and marketplaces may uncover discussions or listings related to your organization. Although risky and time-consuming, this tactic can provide valuable insights into emerging threats, stolen data, or planned cyberattacks.

6. Conduct Regular Cybersecurity Audits.

Regular cybersecurity audits help ensure that your organization's networks and systems are secure. Vulnerability assessments, penetration testing, and security monitoring allow you to identify weaknesses before they are exploited by hackers. By closing potential gaps, you reduce the risk of a breach.

> Journalists, political protestors, and activists can communicate anonymously without fear of persecution

7. Train Employees on Phishing and Cybersecurity.

Employees are often the weakest link in an organization's security chain. Regular training on cybersecurity best practices, such as recognizing phishing emails and using strong passwords, can significantly reduce the chances of a data breach. Emphasizing the importance of securing devices and data is key to safeguarding your organization.

8. Encrypt Sensitive Data.

Data encryption is an essential security measure for both individuals and businesses. By encrypting sensitive data, you ensure that even if it is stolen, it cannot be read or used without the decryption key.

9. Respond to Leaks Immediately.

If you discover that your data has been leaked on the dark web, it is critical to act quickly. Change compromised credentials, inform affected individuals, and engage with cybersecurity experts to mitigate further damage. A strong incident response plan can make a big difference in minimizing the impact of a breach.

Conclusion

The dark web is a complex and multifaceted environment, with both positive and negative aspects. While it offers a platform for privacy, anonymity, and secure communication, it is also a breeding ground for criminal activities. Understanding the risks and taking proactive measures can help individuals and organizations navigate the digital landscape safely.

DECISION REVERSAL RISK:

A HIDDEN THREAT IN BUSINESS STRATEGY

ROBERT MASIGA
Investment Risk Specialist, NSSF

In today's fast-paced business environment, companies are constantly making critical decisions that shape their future. From strategic investments to operational changes, these decisions often carry inherent risks. However, one often overlooked risk is the "Decision Reversal" risk—the danger that arises when organizations reverse significant decisions too quickly or frequently.

Decision reversal, while sometimes necessary, can be detrimental to an organization's long-term strategy and can undermine stakeholder confidence, waste resources, and lead to reputational damage. This article explores what decision reversal risk is, why it occurs, and how organizations can manage it effectively.

What is decision-reversal risk?

Decision-reversal risk refers to the potential negative consequences that occur when a company retracts, alters, or reverses a previously made decision, particularly one that has been widely communicated or implemented. This risk can arise in various contexts, including:

Strategic decisions: Entering or exiting markets, launching new products, or major acquisitions.

Operational decisions: Changes to business processes, systems, or workforce structures.

Financial decisions: Investments, mergers, or divestments.

While decision-making inherently involves some degree of uncertainty, frequent or poorly timed reversals can create confusion, disruption to business operations, and erode trust in the organization and with external stakeholders.

Why does decision reversal occur?

Incomplete or incorrect data.

More often than not, decisions are made with incomplete or inaccurate data/information; and the degree of incompleteness and inaccuracy of data/information influences the quality of decisions made, other factors constant. Although it is difficult to obtain complete and accurate data about the future, if no attempt is made to analyze the available data, with a view to ensuring that it is not only complete, but it is accurate, the risk of reversal of the decision will be high.

Changing market conditions

The business landscape can change rapidly. Economic downturns, technological disruptions, or shifts in consumer behaviour can render a once-sound decision obsolete.

According to the story on https://abc7.com, in 2018, General Motors announced a decision to discontinue production of sedan cars like the Chevrolet Cruze, and shift to SUVs and EVs, citing declining sedan sales. However, by 2023, GM reversed the decision and reconsidered re-entering the compact and affordable vehicle market due to rising competition from Tesla and global economic pressures. Due to the reversed decision, GM lost market share in key segments of affordable cars, missed opportunities as competitors gained ground and suffered costs associated with retooling and re-entering the market.

Additionally, a new policy can be introduced in an organization due to the prevailing situation at that moment, but when the situation changes, it may be necessary to rescind the policy. For instance, during COVID-19, working from home in the NSSF became necessary. However, due to changes in the working environment when normalcy returned, the policy was changed.

Changes in leadership

New leadership often brings new perspectives and priorities, which can lead to reversal of decisions made by previous management. For instance, during President Idi Amin's era of nine years, a number of policies were passed,

including the expulsion of Asians and nationalization, which had negative effects to the economy. However, when President Museveni took power in 1986, he reversed these policies; he allowed Asians to return to the country and repossess their properties. He also privatized various entities that had been nationalized.

While leadership changes can rejuvenate a company, it can also result in instability if decisions are frequently overturned without thorough consideration of long-term impacts.

Regulatory and compliance challenges

Decisions may also need to be reversed due to unforeseen regulatory challenges or changes in legal frameworks. A company expanding into a new geographic region, for example, might reverse its strategy if new regulations make the expansion legally unattainable.

Reaction from stakeholders affected by the decision.

Companies can be quick to reverse decisions based on negative feedback from stakeholders, including investors, customers, or employees. While listening to stakeholder concerns is important, knee-jerk reactions can lead to costly decision-reversal in terms of financial loss and reputation damage.

When making trials during an innovation process

For new initiatives, it is a normal process for several iterations to be performed to test the likely outcome. In the process, several assumptions are made leading to different decisions before the final prototype is agreed. Some of these decisions may be reversed because of new information or new discoveries. Whenever outcomes are negative, assumptions are revisited for changes, which give rise to a decision reversal.

Consequences of frequent decision reversals

Loss of credibility and trust

Repeated decision reversals can create the perception that the organization is indecisive or lacks direction. This can undermine the confidence of investors, employees, and customers. Stakeholders may question the competence of leadership and the organization's ability to execute long-term strategies. For example, in 2019, Tesla announced that it would close many of its brick-and-mortar stores and shift all sales to an online-only model; in part to lower the prices of its vehicles.

Following criticism from customers who preferred physical stores and concerns about service accessibility, Tesla reversed its decision just days later. It decided to keep more stores open than initially planned and increased car prices to cover operational costs. This abrupt reversal created confusion among customers and investors, raising questions about Tesla's strategic clarity. The rapid U-turn led to criticism about the company's decision-making process and communication practices, which risked long-term brand trust.

Wasted resources

Some decisions involve commitment of significant financial and human resources. Reversing such a decision can have significant financial loss and reputation damage. A company that reverses a major technology upgrade after implementing it may face additional costs to undo the changes and reinstate the previous system. For example, Smart Telecom – Digital Platform Scale-Back: Smart Telecom invested in digital service platforms, including mobile money and data services, to compete with leading telecom companies. It introduced promotions and packages aimed at increasing user adoption of its digital services. Despite the initial investment, the decision reversal emanated from Smart Telecom's continued operational challenges, limited market reach, and financial losses. The digital services struggled to gain traction against established competitors like MTN and Airtel. By 2021, Smart Telecom exited the Ugandan market, effectively rolling back its digital services and discontinuing its investments in technology upgrades.

Also, Nakumatt Supermarkets suffered retail management system rollback. Nakumatt had to reverse its decisions despite having invested in a digital retail management system to optimize inventory management, enhance the customer shopping experience, and support its loyalty program. According to the BusinessFocus, the upgrade was intended to streamline operations across its regional outlets, including those in Uganda.

However, with deepening of its financial troubles, the company struggled to maintain the system due to cash flow problems. The inability to meet vendor payments and the closure of outlets across Uganda and other East African countries forced the supermarket chain to roll back the digital system and revert to manual operations in some locations. The company eventually exited Uganda in 2017, and the system upgrade was effectively abandoned.

Operational disruptions

Frequent changes in direction can disrupt workflows, reduce productivity, and lower employee morale within the organization. Employees may become confused about priorities, leading to inefficiencies and disengagement. Operational plans may be delayed or abandoned entirely, compromising the organization's ability to achieve its goals.

For instance, in 2011, J.C. Penney CEO Ron Johnson implemented a "Fair and Square" pricing strategy, eliminating discounts and coupons in favor of everyday low prices to simplify the shopping experience. The strategy backfired as J.C. Penney's customers, accustomed to heavy promotions, rejected the new pricing model. Sales plummeted, and the company reversed its decision in 2013, bringing back discounts and promotional pricing. The "Fair and Square" pricing strategy by J.C. Penney's, which damaged its relationship with customers and investors, resulted in billions of dollars in losses and ultimately Johnson's ousting as CEO. The company struggled for years to recover from the effects of this decision.

Reputation damage

When a company reverses high-profile decisions, it risks damaging its reputation. Publicized U-turns can be seen as signs of weak leadership or poor strategic planning, which can harm the institution's image in the public. Competitors may seize the opportunity to portray themselves as more stable and reliable. A case in point is the British Government's U-Turn on Tax Cuts (2022): The

UK government, under Prime Minister Liz Truss, proposed sweeping tax cuts for the wealthy without explaining how the cuts would be funded. The proposal, part of a broader "mini budget," was intended to boost economic growth.

However, after market turmoil-a sharp fall in the value of the pound, and strong political and public backlash, the government quickly reversed key elements of the budget, including the most controversial tax cuts. The decision reversal severely damaged the government's credibility, leading to significant political instability, including Truss, the then prime minister to resign. The reversal also eroded investor and public confidence in the government's economic management.

Managing Decision Reversal Risk

To minimize the potential downsides of decision reversals, organizations should adopt a proactive approach to risk management. Here are some key strategies to mitigate this risk:

Invest in thorough decision-making processes

Sound decision-making starts with having the right data, validating it, and analyzing it to gain better insights. Organizations should implement structured decision-making frameworks that ensure all relevant factors—market trends, financial projections, regulatory risks, and stakeholder impacts—are carefully considered. Stress-testing decisions under various scenarios can help identify potential pitfalls before committing resources.

Improve communication and transparency

When a decision needs to be reversed, transparency is critical. Clear communication with stakeholders about why the reversal is necessary, what steps will be taken to mitigate the impact, and what the organization has learned from the experience, can help maintain trust. Internal stakeholders, such as employees, should be involved in discussions early to minimize confusion and operational disruptions.

Establish contingency plans

Having contingency plans in place allows organizations to pivot more smoothly when a decision reversal is unavoidable. For example, if a company is launching a new product, having backup strategies to address potential market shifts can reduce the risk of an abrupt reversal and the accompanying negative effects.

Foster organizational agility

While decision reversals should not be frequent, organizations need to remain agile enough to adapt when necessary. Companies that cultivate a culture of flexibility and responsiveness are better equipped to handle reversals without losing momentum. Empowering teams to make rapid adjustments when circumstances change can help manage the fallout from a reversed decision.

Monitor and learn from past reversals

Decision reversals offer valuable learning opportunities. Organizations should track past reversals, analyze the reasons behind them, and use those insights to improve future decision-making processes. A "lessons learned" review can prevent the same mistakes from being made again and improve the organization's resilience.

In conclusion, decision reversal risk is an inherent aspect of the business world, especially in an era of rapid changes. However, frequent and poorly managed reversals can have serious consequences for an organization's credibility, operations, and financial health. By adopting sound decision-making processes, enhancing communication, and fostering an agile culture, organizations can minimize the negative impact of decision reversals and maintain the confidence of their stakeholders.

Breathing life into work...

Set yourself apart. Create uncontested market spaces with.....

talis
CONSULTS

Reach us at;

info@talisconsults.com
+256 393 246029
+256 701 210401

ENQUIRIES

Plot 6/8, Nakasero Lane,
First Floor, Kisozi House
Kampala, Uganda

ADDRESS

www.talisconsults.com

BALANCING AMBITION WITH YOUR RISK PERSONALITY

ANDREW BUKENYA
Senior Manager, Enterprise Risk Management,
MTN – Uganda

Ambitions drive us—they inspire us to build successful careers, live fulfilling lives, secure our retirement, and leave lasting legacies for our families. We strategize, act, and hope for the best. Yet, life often throws unforeseen challenges our way. This isn't about giving in to fate but about understanding the limits of our ability to predict or control outcomes. These uncertainties—the essence of risk—shape our journeys in unexpected ways.

To dispel the outdated notion that risk should always be avoided, it's time to ask a crucial question: how far are you willing to go to achieve your ambitions? Answering this forces us to consider our natural tendencies, deliberate choices and prepare for uncertainty. The interplay between ambition and risk personality is not just a reflection of our goals but also of how we approach achieving them. Balancing these two forces is key to sustainable success.

Ambition is the driving force behind human progress. It defines our aspirations, influences our decisions, and determines the extent of our achievements. From pursuing personal milestones to striving for societal impact, ambition gives direction to our actions. For many, ambition is a natural motivator, pushing them to seize opportunities and overcome challenges.

However, ambition is not a one-size-fits-all trait. Some individuals are highly ambitious, setting bold and often challenging goals, while others may exhibit more modest or reserved aspirations. Highly ambitious individuals are typically relentless in their pursuit of success, but they may face risks such as burnout, overcommitment, or unrealistic expectations. On the other hand, those with limited ambition may avoid risks altogether, leading to stagnation, missed opportunities, or unfulfilled potential.

Striking the right level of ambition is essential for achieving meaningful goals without compromising well-being. Ambition is not inherently positive or negative—it depends on how it is harnessed and balanced against other factors, including one's personality and risk tolerance.

Risk personality refers to an individual's inherent approach to uncertainty. It significantly influences how they make decisions, respond to challenges, and pursue their ambitions. Broadly speaking, people can be categorized as either risk-averse or risk-seeking:

Risk-averse

Individuals tend to prioritize safety and avoid uncertainty. They often choose stable and predictable paths, and may shy away from ambitious goals that carry significant risks. While this cautious approach minimizes exposure to failure, it may also limit opportunities for growth and achievement.

Risk-seeking

Individuals on the other hand, embrace uncertainty and are more willing to take bold actions to achieve their goals. They are often associated with innovation and breakthroughs but may expose themselves to unnecessary risks or fail to evaluate potential downsides adequately.

Personality traits, life experiences, and even cultural influences shape our risk tendencies. Interestingly, ambition and risk personality are deeply intertwined. Highly risk-averse individuals may exhibit less ambition because

they fear the uncertainties involved, while risk-seekers may sometimes pursue overly ambitious goals without adequate preparation.

Both extremes come with challenges:

- Being overly cautious can lead to missed opportunities and unfulfilled potential.
- Being excessively ambitious or reckless can result in burnout, financial loss, or strained relationships.

To achieve sustainable success, it is essential to balance ambition with one's risk personality. This balance ensures that goals are pursued thoughtfully, minimizing unnecessary risks while seizing opportunities for growth. Here are practical ways to achieve this balance:

1. Self-awareness

Understanding your ambition level and risk personality is the first step. Reflect on your natural tendencies—are you more risk-averse or risk-seeking? Are your ambitions aligned with your risk tolerance? Tools such as personality assessments or feedback from trusted peers can provide valuable insights into your decision-making style.

2. Set Realistic Goals

Ambition is most productive when paired with realistic and measurable goals. Overly ambitious targets can lead to frustration or failure, especially for risk-seeking individuals. Similarly, risk-averse individuals should ensure that their ambitions are grounded in reality and achievable within their resource constraints.

3. Build a Support System

Collaboration with others can help bridge gaps between ambition and risk personality. For instance, risk-averse individuals can benefit from mentors or partners who encourage them to take calculated risks, while risk-seekers may need advisors to provide caution and different perspectives.

4. Upskill and Prepare

Education, training, and experience empower individuals to manage risks effectively. For example, a risk-averse person might feel more confident pursuing ambitious goals if they have the skills and knowledge to mitigate potential challenges. Risk-seeker, on the other hand, can benefit from learning structured approaches to evaluate and manage risks.

5. Embrace a Risk Philosophy

A risk philosophy serves as a guiding framework for making decisions and pursuing ambitions. It encourages individuals to align their actions with their values and long-term goals. For businesses, cultivating a risk-integrated culture ensures that employees' personal tendencies align with the organization's objectives, creating a cohesive and sustainable approach to risk-taking.

6. Iterate and Adapt

Balancing ambition and risk personality is not a one-time effort—it requires continuous evaluation and adjustment. As circumstances change, be open to recalibrating your goals and strategies to stay aligned with your evolving priorities and environment.

Ambition and risk personality are not opposing forces but complementary elements of personal and professional growth. By understanding and balancing these traits, individuals and organizations can pursue meaningful goals while navigating uncertainties effectively.

So, what's your risk personality? Are you willing to adapt it to achieve your ambitions? Striking the right balance between ambition and risk is not just a strategy for success—it's a philosophy for living a purposeful and fulfilling life.

CYBERSECURITY:

A STRATEGIC APPROACH TO PROTECTING DIGITAL ASSETS

SHEBA AINEMBABAZI
Cybersecurity Professional, Umeme Ltd

In today's digital world, the importance of cybersecurity cannot be overstated. As organizations increasingly rely on online systems to conduct business, they must adopt robust strategies to manage the ever-growing risks associated with cyber threats. From malware to insider threats, businesses are constantly vulnerable. A risk management perspective in cybersecurity offers a structured approach to identifying, assessing, and mitigating these risks, ensuring business continuity and protecting critical assets. Let's explore the key elements of cybersecurity risk management, from identification to mitigation.

1. Risk Identification with Advanced Tools and AI Integration

One of the primary steps in risk management is identifying potential threats. Traditionally, this has been done using tools such as antivirus and anti-malware software. However, with the sophistication of modern cyber threats, it's crucial to integrate advanced solutions powered by Artificial Intelligence (AI). AI-backed cybersecurity tools are able to detect and counter new threats in real-time, providing a more proactive defense. For larger organizations, especially those with many employees operating online, implementing a Security Operations Center (SOC) is essential. SOCs allow for the constant monitoring of networks and systems, ensuring that any abnormal activity is detected before it can escalate into a significant problem.

2. Speed in Threat Detection and Risk Assessment

A key factor in both risk identification and risk assessment in cybersecurity is the speed at which threats are detected. The faster a potential cyber threat is identified, the faster it can be neutralized, minimizing potential damage. Risk assessment involves evaluating the potential impact of threats on your assets. By swiftly identifying risks, businesses can prioritize which threats require immediate action, thereby preventing data breaches or significant operational disruptions.

In 2020, the SolarWinds cyberattack revealed how a single weak spot could affect hundreds of businesses and even U.S. government agencies. Attackers used a normal software update to slip into SolarWinds IT infrastructure unnoticed, accessing critical systems for months. This event shows how vital it is to detect threats quickly and have strong systems in place to block advanced attacks.

3. Risk Mitigation: The Most Critical Step in Cybersecurity

While identifying and assessing risks are important, risk mitigation is where organizations take active steps to prevent damage. Implementing robust risk mitigation strategies is vital for protecting sensitive data and ensuring operational integrity.

Let's look at three crucial risk mitigation strategies for effective cybersecurity.

i) Zero Trust Model: A Defense Against Internal and External Threats

One of the most effective strategies in modern cybersecurity is adopting a Zero Trust approach. This principle assumes that every person or device with access to a system, including IT teams, is a potential vulnerability. By treating all users as possible threats, companies can implement multiple layers of security, such as multi-factor authentication (MFA) and role-based access controls. Even senior management, including the head of the cybersecurity team, must follow these protocols. This approach ensures that even if one user's credentials are compromised, unauthorized access to the network is prevented. Though it can seem inconvenient, Zero Trust remains one of the most powerful tools to defend against cyberattacks.

ii) Cloud-Based Systems: Enhancing Security Through Controlled Access

For larger companies or those with remote workforces,

leveraging cloud access systems is a game-changer. When employees are required to access data through a centralized cloud platform, organizations gain better control over the flow of information. This means that any data uploaded or accessed is authorized and monitored. Additionally, by limiting access to sensitive data to only those employees who need it, businesses can reduce the risk of malware or phishing attacks, which often originate from casual web browsing on personal devices.

iii) Dedicated Work Devices: Limiting the Attack Surface

Another crucial risk mitigation strategy is providing employees with dedicated work devices, such as laptops or tablets that are strictly for business use. Limiting the number of users on a device reduces the risk of external vulnerabilities being introduced into the system. Moreover, having dedicated devices allows cybersecurity teams to monitor activity 24/7, ensuring real-time detection of suspicious activities. This way, companies can control the security of their network more effectively, reducing the risk of cyberattacks.

iv) Building a Fortress: Layered Security for Maximum Protection

In addition to the Zero-Trust model, cloud-based systems, and dedicated work devices, organizations can create a cybersecurity infrastructure that operates like a fortress. The layered security approach ensures that even if one layer is breached, other measures are in place to prevent a full-scale attack. These strategies make it incredibly difficult for cybercriminals to infiltrate a company's systems or steal sensitive information.

Consequences of Cyber Attacks

Cyberattacks can ripple through entire industries, causing operational chaos and exposing sensitive data.

Take for example the Change Healthcare ransomware attack in 2024. The BlackCat gang infiltrated systems, stealing 4TB of patient data and paralyzing billing and payment operations. This breach disrupted nearly 40% of medical claims processing in the U.S, leaving hospitals, insurers, and patients scrambling. One critical weakness was the absence of multifactor authentication on remote servers, which made it easier for attackers to gain access. This incident underscores the devastating effects of cyberattacks and highlights the need for strong access controls and robust security measures to safeguard critical infrastructures.

Conclusion

Cybersecurity is not just an IT issue—it's a foundational part of protecting personal and organizational interests. By implementing strategies such as the Zero Trust model, leveraging secure cloud-based systems, and using dedicated work devices, organizations can build a resilient defense against cyber threats. A layered approach to security ensures that even if one protective measure fails, others stand ready to prevent or mitigate the impact of an attack.

DIVERSIFICATION:

AN IMPORTANT ASPECT OF INVESTING.

ANDREW MWIMA
Financial markets consultant and a practitioner in the Capital Markets Industry.

Reagan is a young professional; intelligent, hardworking and highly accomplished. Many years ago; he approached an investment advisor who happens to be a friend. He was keen to start investing in stocks; he had a desire to buy shares in a company that had gained a return of over 200% in a 3-year period. The advisor was in agreement with Reagan but recommended that he considers spreading his money across other companies (Diversification) as well. Reagan didn't heed this advice though and invested in the same stock for almost 5 years; his portfolio lost 80% of its value because of that grave mistake.

Diversification is one of the core principles of sound investment strategy, and it is particularly important as a risk management tool. The main goal of diversification is to reduce the overall risk of a portfolio by spreading investments across different assets, sectors, geographic regions, or investment styles. The rationale behind diversification is that different assets or asset classes often respond differently to the same economic event or market condition. By holding a variety of assets, an investor can reduce the chances of significant investment losses, since the likelihood that all assets in their investment portfolio will decline in value at the same time, is low.

Here's how diversification works as a risk management tool:

a) Diversification by asset classes

If you had UGX100M, you could choose to invest 60% in fixed income, 30% in stocks and 10% in real estate. Fixed income is mainly influenced by interest rates, an increase in interest rates may disadvantage a person who has already fixed his money. Equities are mainly driven by business cycles; good times often result into gains and the reverse is true, while real assets are inflation hedged and provide average but stable returns. Each asset class may be affected by factors which do not necessarily affect the other asset classes or vice-versa; consequently, the losses in one asset class will be offset by the gains from the other assets or vice-versa.

b) Diversification by sectors

Different sectors have different risks and return perspectives. For example, oil and gas companies experience more volatility than consumer goods companies-the price of soap is less volatile than the price of oil. You need to avoid concentration in one or a few sectors (e.g., banking, technology, energy). Instead, spread investments across a variety of industries, such as consumer goods, oil and gas, healthcare, and banking, insurance, telecom, etc.

c) Diversification by geographical location

Invest in both domestic and international markets

Global diversification can help protect against the risks of relying too heavily on the performance of a single country's economy. Imagine an investor who had only stocks and bonds in Ukraine, his investments must be strongly impaired now. However, geographic diversification increases risks like currency and information asymmetry (limited timely access to information).

Time Horizon Diversification

Liquidity is a major factor in investment; different assets have different investment periods. The investment period for real assets and equities is often 10 years while fixed income has a spectrum from 3 months to greater than 20 years. An individual has to invest with different time horizons in mind. This can mean holding a mix of short-term, medium-term, and long-term investments to balance liquidity needs and growth objectives.

Importance of diversification

i) Reduction of Specific Risk

Specific/Unsystematic risk refers to the risk that is specific to a particular company, sector, or industry (also called "idiosyncratic risk"). Examples include management issues, regulatory changes, or product recalls.

By diversifying across different companies, industries, sectors, or asset types, an investor reduces the impact of any single event on the overall portfolio. For example, poor performance in the technology sector might be offset by gains in the healthcare or energy sectors.

ii) Lowering the Impact of Market Volatility

Markets can be volatile, with asset prices fluctuating based on macroeconomic factors like interest rates, inflation, geopolitical events, and investor sentiment. Diversification helps by ensuring that not all investments are subject to the same risks at the same time.

For example, when stock markets are underperforming due to economic slowdowns, bonds or real estate may perform better, thus helping to cushion the overall portfolio against losses.

iii) Exposure to Different Sources of Return

Diversification allows investors to tap into a wider range of return opportunities across different markets or asset classes. Stocks, bonds, real estate, commodities, international investments, and alternative assets like private equity or hedge funds may each respond to market conditions differently.

For instance, equities might perform well in periods of economic growth, while fixed-income securities (bonds) tend to do better in times of economic uncertainty.

iv) Reducing Correlation

One of the key concepts behind diversification is reducing correlation among the assets in a portfolio. Assets that have low or negative correlations with one another provide greater diversification benefits.

For example, Ugandan stocks and foreign stocks might not always move in the same direction, or even if they do, the magnitude of the moves could be different. Similarly, stocks and bonds often have an inverse relationship, especially during times of market stress, which can help offset equity losses.

v) Enhancing Risk-Adjusted Returns

Diversification allows an investor to improve their risk-adjusted returns; the returns earned per unit of risk taken. A well-diversified portfolio may not have the highest possible return in any given year, but it aims to smooth out fluctuations in performance and reduce the likelihood of large losses.

vi) Enables access to international markets

By investing across countries and regions, an investor can mitigate the risks associated with a single country's economy.

For example, the economic or political instability in one country may be offset by the stability or growth in another region, such as emerging markets or developed economies in Europe and Asia.

Moreover, global diversification exposes investors to growth opportunities in different parts of the world, which may not be fully correlated with the performance of the investor's domestic market.

vii) Limiting the Impact of "Black Swan" Events

Black swan events, or rare and unpredictable occurrences, can have a disproportionate effect on investments. While diversification cannot eliminate the risk of such events, it can help mitigate their impact. For example, a catastrophic event that severely affects one sector (e.g., a technology crash) may be less damaging to a diversified portfolio if it has significant exposure to other sectors such as healthcare, utilities, or commodities.

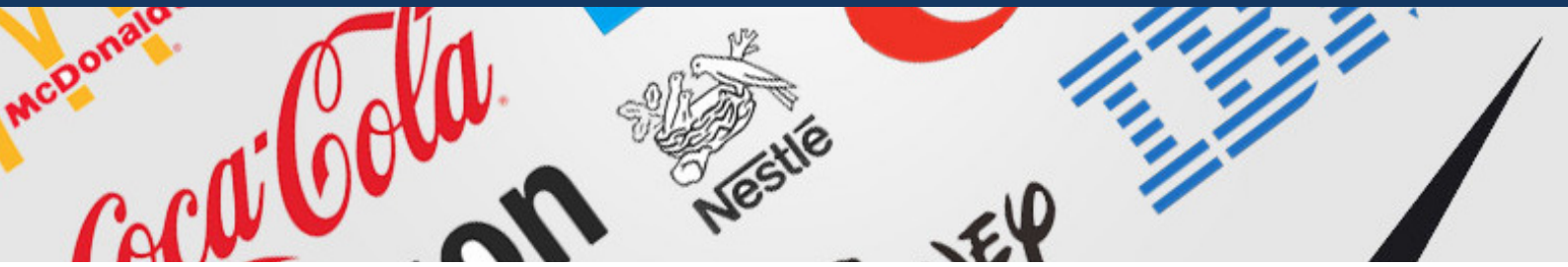
Conclusion

Diversification helps reduce the risk of large losses in a portfolio by spreading investments across a variety of asset classes, sectors, and geographical areas. While it can't eliminate all types of risk, such as systemic risk (market-wide risk), it is an effective strategy to minimize unsystematic risk and smooth out returns over time. A well-diversified portfolio is more likely to perform steadily through market fluctuations, giving investors a better chance to achieve long-term financial goals without facing significant losses during periods of market stress.

BRAND REPUTATION MANAGEMENT:

TRAVERSING CHALLENGES IN A DIGITAL ERA.

MIKE KYEYUNE
Product Development Analyst, NSSF



Brand reputation is one of the most valuable assets an organization possesses. In an increasingly interconnected and fast-paced world, managing and safeguarding this intangible yet critical asset has become more challenging than ever before. Negative publicity, social media backlash, or even minor customer dissatisfaction can have long-lasting impacts on a brand's credibility and market position. Effective brand reputation management is, therefore, essential for organizational success and resilience.

A brand is much more than just a logo or name; it represents the company's identity, values, and perception of a product in the minds of consumers. It is a comprehensive combination of elements that collectively distinguish a business or product from its competitors. In principle, a brand is the promise that a company makes to its customers, which is reflected in everything it does; from the services and products it sells, to how it communicates with its audience. The mismanagement or criticism of the brand could easily lead to the collapse of a company.

In 2008, Top Gear, a TV show on BBC where the latest models of cars are reviewed, featured a Tesla Roadster electric car. The presenters portrayed the car as having significant battery issues, including running out of power during a test drive. This show accumulated over a million views on YouTube and other social media platforms. This affected the Tesla electric car manufacturer's reputation, and the brand took reputational damages as users and admirers of the car started doubting the vehicle's functionality, which consequently affected the company's share price.

Such incidents if not managed, can affect a company's success. Brand reputation management has increasingly become the most critical aspect of maintaining business success, especially in today's fast-paced and digitally connected world. A brand's reputation influences consumer trust, loyalty, and purchasing decisions, making it essential for companies to invest in strategies that safeguard and promote their image.

So, what is brand reputation management (BRM)?

These are strategies and actions a company takes to monitor, influence, and protect its reputation in the eyes of the stakeholders; this includes monitoring the brand health, public relations, crisis management, etc., all aimed at ensuring that the brand maintains a positive perception among stakeholders.

Why Brand Reputation Management is important

i) Building Customer's trust and loyalty

Due to the fact that consumers have endless alternatives in the market, this coupled with their ever-shifting tastes and preferences, having a solid reputation fosters loyalty and attracts customers. Therefore, positive reviews from consumers, consistent quality in service and products offered and transparency, are key to building trust and loyalty among customers.

ii) Maintaining a competitive advantage

A strong brand reputation provides a competitive edge in a crowded market. Let's take an example of Colgate and Shell; most people in rural areas generally refer to any toothpaste or petrol station as Colgate and Shell, respectively. All the other brands are shadowed, and this has given Colgate and Shell a competitive advantage over others.

iii) Crisis prevention and damage control (mitigating risks)

Every brand faces challenges; these could be as a result of poor public relations, social media criticisms, etc. Such incidents test the resilience of a brand. Effective reputation management in this case would include preparing for potential crises and having a plan in place to mitigate damage. Usually, a proactive approach helps prevent negative events from spiraling out of control.

iv) Influence on purchasing (driving growth)

During the Covid-19 pandemic, COVIDEX a locally manufactured drug, took the market by storm even before Uganda National Drug Authority approved it. This means, customers today are highly influenced by recommendations from friends and family more than any form of advertising. Therefore, maintaining a strong brand in the eyes of consumers is highly influenced by reputation of brands.

What are some of the key strategies for Brand reputation Management?

i) Content marketing and thought Leadership

Publishing insights, articles, high-quality social media contents that resonate with the target customers helps position a brand in the market. When presenters on Top Gear tarnished Tesla brand, Tesla tried to sue BBC but was never successful. However, they turned to creating social media contents and publications about electric vehicles and this changed consumers perception about Tesla. Blogs, whitepapers, case studies, etc. contribute to building a strong brand and fosters trust and credibility over time, which was the case with Tesla.

ii) Monitoring and listening

Reputation management always has the element of listening and monitoring what people are saying about the brand. Companies have developed algorithms that help to listen or monitor online conservations, contents and blogs published about them. Netflix, a leading online movie platform for example, consistently picks up any information about them on social media, media houses, etc. Monitoring and listening helps businesses stay informed about what is being said about them in real-time.

iii) Responding to customer's feedback

Engaging with customers on both positive and negative feedback, is important. Companies should acknowledge positive comments and thank customers for their support. Negative feedback should also be addressed promptly and professionally. Offering solutions to complaints and turning a dissatisfied customer into a satisfied one can significantly improve the brand's image.

iv) Influencer partnerships

Collaborating with influencers who align with the brand's values can be a powerful way to enhance its reputation. Influencers can help extend the reach of the brand's message and provide social proof. However, these partnerships should be approached carefully, ensuring that the influencer's image aligns with the brand's reputation. For example, Cristiano Ronaldo's removal of Coca-Cola bottles from a 2020-press conference had a brief negative impact on the company's market value, but no direct effect on sales; the share prices dropped by 1.6% and market value reduced from $242bn to $238bn (ESPN).

v) Building a positive online presence

A well-maintained website and active social media profiles are essential components of a brand's reputation management. Regularly updating contents on the websites, conveying new developments through social media posts, having meaningful engagement with followers, and showcasing customer testimonials and success stories, can help strengthen the brand's image. We see organizations like National Social Security Fund, Telecom companies (Airtel and MTN) are always engaging customers on their social media handles by answering their complaints.

vi) Corporate Social Responsibility (CSR)

In today's social landscape, many consumers expect brands to take an active role in addressing societal issues. Companies that invest in environmental sustainability, support charitable causes, and promote ethical practices are viewed more favorably.

Let us take an example of the NSSF Kampala Hills Run and MTN marathon; these have raised funds to renovate government schools, which is an important contribution to societal needs. Additionally, the NSSF recently launched an ESG initiative to show commitment to protecting the environment and promoting good governance. A strong CSR strategy can reinforce a positive reputation and establish emotional connections with consumers and stakeholders.

What are some of the common mistakes in brand reputation management?

i) Negative feedback

One of the biggest mistakes organizations make is ignoring negative comments and customer reviews about products or services. Whether it's on social media, TV or a review site, ignoring criticism can lead to further dissatisfaction and a deteriorating reputation.

In mid-2011, Netflix ignored complaints from a negative pressure group when the company announced, without prior warning, that it would be splitting company services; that is the DVD rental by mail and live-streaming films, while raising up their prices. By September same year, when Netflix rolled out the changes, it had lost 800,000 subscribers and the share price had dropped from $300 to $50 on Wall St. The managing director at that time learned his lesson, listened to his customers, revised the company decision and apologized to the customers.

ii) Inconsistent messaging

A company that sends mixed communications/messages can confuse consumers and diminish trust and loyalty. Consistency across all channels, including advertising, social media, customer service, and corporate communications, is essential for maintaining a strong reputation; that is why companies maintain uniform communications across all their media channels and branches.

iii) Lack of transparency

Customers value honesty. Companies and organizations that try to hide their mistakes or spin negative situations face backlash. It's important to acknowledge issues openly, take responsibility, and outline steps to resolve them. Transparency helps build credibility and prevents rumors from spreading. In 2018, the CEO of Starbucks came out openly and apologized publically to the men who were wrongly arrested and harassed in one of its outlets.

In conclusion

Brands are much more than just names and logos; this is something that companies need to protect jealously because it's a promise that encapsulates everything a company stands for. Brand reputation management is not just about protecting a brand from negative publicity, it's about building a foundation of trust, credibility, and authenticity with customers. By investing in proactive reputation management strategies, companies can protect their reputation, foster customer loyalty, and position themselves for long-term success.

THE FUTURE OF CYBER SECURITY LIES IN CONFIGURING THE HUMAN BRAIN

RODNEY HOOD ADRIKO
Head of Cyber Security Assurance, Centenary Bank

No matter how much technology advances, the human brain remains one of the most significant assets in cyber security, yet it is also one of the most exploited vulnerabilities. While organizations invest in advanced technologies like firewalls and encryption, a single careless action by an employee such as clicking on a malicious link can compromise even the most robust defence systems.

This raises a critical challenge: how can we reconfigure the human brain to align with the demands of cyber security? How can we attempt to configure something so complex and abstract that the creator provided no manual for?

The answer lies in fostering a mindset where every individual sees themselves as a crucial component of the organization's cyber security fabric. By reshaping habits, attitudes, and awareness, organizations can transform their workforce into a resilient line of defence to develop them into the strongest link in the cyber security chain.

Cyber attackers have often exploited psychological tendencies, leveraging traits like trust, urgency, and curiosity to manipulate their targets. For example, phishing emails may appear to come from a trusted colleague or contain fake deadlines designed to prompt quick and thoughtless actions from the victim. Understanding these vulnerabilities in human cognitive abilities is key to equipping employees to recognize and guard against such threats.

Through tailored training and awareness, organizations have an opportunity to reprogram human responses. Regular awareness training on secure practices like spotting phishing attempts, setting secure passwords, and recognizing suspicious activity can help in recalibrating employees' instincts. By exposing staff to simulated threats in controlled settings, they can become better equipped to respond effectively to real-world attacks.

This learning can also be enhanced through incorporating gamified elements to further drive the message home. Humans are naturally drawn to competition and rewards, so offering points or incentives for correctly identifying threats can help ingrain security conscious behaviour.

An additional step could involve recognizing and rewarding employees who demonstrate exceptional vigilance.

All these fosters a culture where proactive security practices are valued and celebrated in the organisation. Cyber security is not just about rational processes—it is deeply emotional and as such, psychological factors such as fear, when managed correctly, can be a motivator for a good cyber security culture. Highlighting real-world examples of breaches to staff emphasises what is at stake and at the same time, empowers them with the tools and knowledge to prevent similar incidents.

A sense of shared responsibility, where individuals understand how their actions affect the broader organization, can strengthen staff commitment to cyber security. Although technology plays a significant role in cyber security, it is the human firewall (the collective vigilance of employees) that often determines the outcome of an attack.

Clear communication, consistent messaging, and straightforward policies are important in aligning employee behaviour with security objectives. Employees should be encouraged to question unusual requests or communications, even if they appear to come from trusted sources. This scepticism can disrupt the success of tactics like social engineering, which rely on exploiting trust and familiarity.

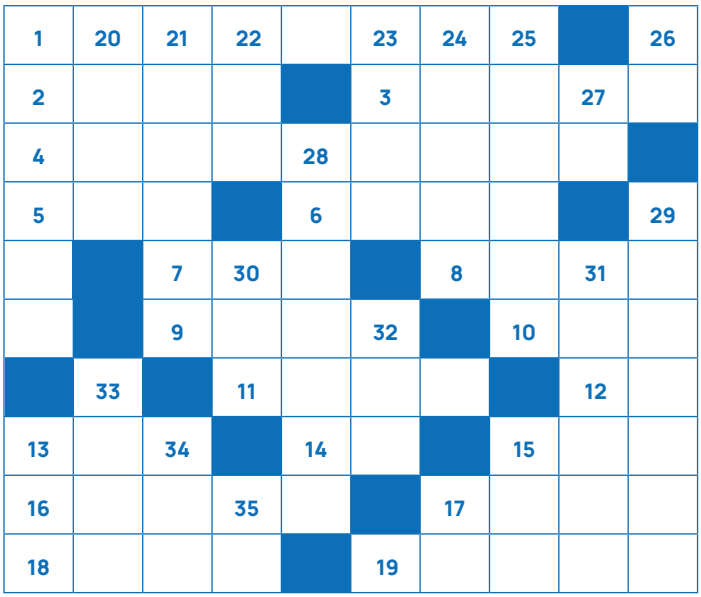
Despite these efforts, challenges persist. Overconfidence can lead some employees to underestimate threats, while others may resist new security practices. These are barriers that must be addressed through continuous engagement and clear communication about the importance of adherence to security measures.

The success of reengineering the human brain through continuous awareness has been realised and is evident in real-world cases. Reduction in phishing incidents can be attained through integrating awareness programs, real-time tests, and reward systems for vigilance. This allows employees to become more alert, and promptly report phishing attempts, preventing potential breaches.

As technology and cyber threats evolve, so must human behaviour. Configuring the human brain for security is an ongoing process with no clearly defined start and end points. Artificial Intelligence and behavioural analytics can complement human vigilance by identifying anomalies and tailoring training to individual needs. By fostering awareness, encouraging proactive behaviour, and leveraging emotional and cognitive insights, organizations can transform their workforce into an indispensable layer of defence.

In nutshell, the battle against cyber threats is not just about systems and software—it is about people, their decisions, and their actions. Empowering individuals to take ownership of their role in cyber security is the most effective way to build a resilient organization in the digital age.

PUZZLE ISSUE NO.9



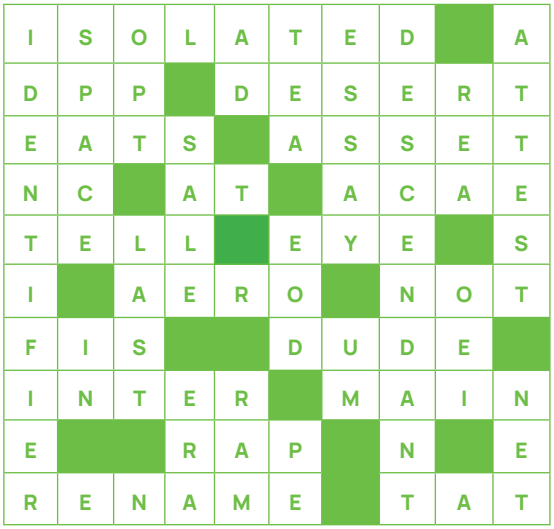
ACROSS:

1. A natural desire to satisfy a bodily need, 8
2. Small room in which a prisoner is locked up, 4
3. Rigid structure that surrounds something such as a picture, 5
4. Moves from one place to another, 9
5. Trade association for American and international investment companies, including mutual funds, closed-end funds, exchange traded funds, and unit investment trusts, abbr.3
6. A greenish blue colour which is one of the primary subtractive colours, complementary to red, 4
7. Denoting an unspecified member of a series of numbers, 3
8. Take part in commercial trading of a particular commodity, 4
9. A deep black powdery or flaky substance consisting largely of amorphous carbon, 4
10. Dermatology, Venereology and Leprosy, abbr.3
11. A wide way leading from one place to another, 4
12. A salesperson with primary day-to-day responsibility for an ongoing business relationship with a customer, abbr.2
13. New metric for physical activity tracking, associated with reduced risk of all-cause and cardiovascular mortality, abbr.3
14. Note that acknowledges the receipt of goods by a carrier (usually a lorry or truck), abbr.2
15. Set up (equipment or a device or structure), typically in a makeshift or hasty way, 3
16. A book of maps or charts, 5
17. Long, rounded piece of wood or metal, 4
18. Communicate information to someone in spoken or written words, 4
19. Perfect happiness; great joy, 5

DOWN

1. Engaging or ready to engage in physically energetic pursuits, 6
13. Touch quickly and gently with the flat of the hand, 3
15. A metric used to evaluate the performance of the investment, abbr. 3
17. Abbreviation (in writing) of plural, 2
20. Rule utilized by physicians to avoid further testing for pulmonary embolism in patients deemed to be at low-risk, abbr.4
21. Large areas of flat land with few trees, 6
22. Debt instrument, usually a bond, where the payout is based on the underlying entity, abbr.3
23. Full of uncertainty; doubtful, 4
24. Walk in a specified way, 5
25. Obtained (money) in return for labour or services, 6
26. Word adopted from Latin originally meaning 'apart' (as in separate) or meaning 'without' (as in secure) prefix, 2
27. Title used before a name of any woman regardless of her marital status, 2
28. Institutions for educating children, 7
29. Asserts that someone has done something illegal or wrong, typically without proof, 7
30. Defines the purpose and structures of a project, committee, or negotiation, to work together to accomplish a shared goal, abbr. 3
31. Helps or benefits, 6.
32. Dark, thick flammable liquid distilled from coal, consisting of a mixture of hydrocarbons, resins, alcohols, etc. 3
33. Doing something or taking place after the expected time,4
34. Feeling unwell, 3
35. Adjective suffix. meaning 'relating to', 2

SOLUTION TO ISSUE NO. 8



BEERA APPDATED

*Update your **NSSF Account Details.**

National ID | Phone Number | Email | Employment Records | Dependants (Spouse/Children)

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

Visit **www.nssfgo.app** Dial ***165*26#** (MTN only) Visit the **NSSF Branch** near you

For more information, call **0800 286 773 (Toll-Free)**, WhatsApp **+256 784 259 713**
or email **customerservice@nssfug.org** | *T&Cs Apply.

NSSF
a better life