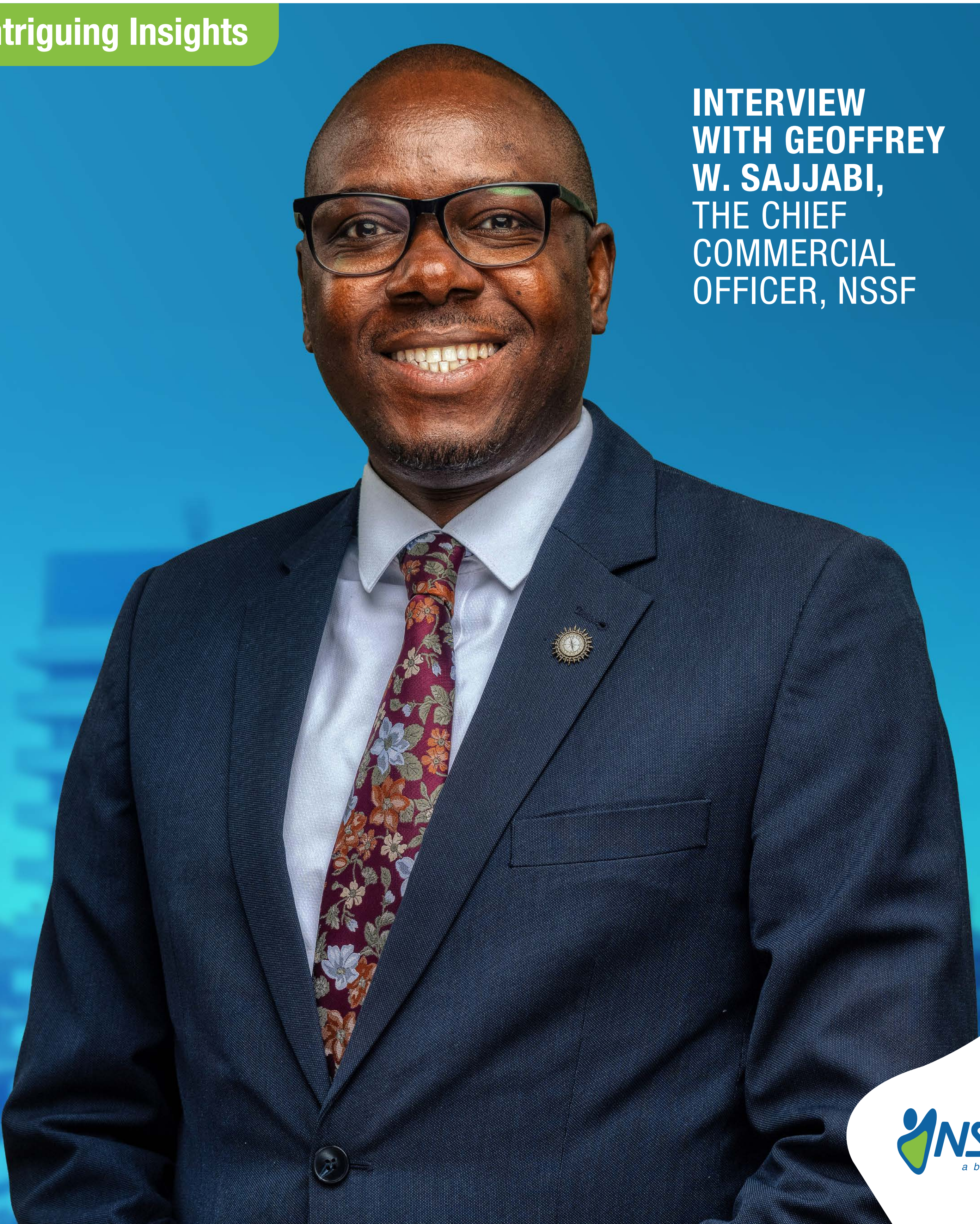
ISSUE 7 | JUNE 2023

The RiskEcho

Intriguing Insights



INTERVIEW WITH GEOFFREY W. SAJJABI, THE CHIEF COMMERCIAL OFFICER, NSSF

NSSF
a better life

FOREWORD

Welcome to the seventh issue of The Risk Echo magazine, a centerpiece of enterprise risk management. As the global landscape continues to face unprecedented challenges, the ability to effectively identify, assess, and mitigate risks has become paramount for organizations, governments, and individuals alike.

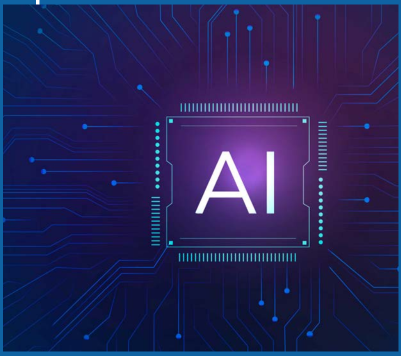
In an era marked by rapid technological advancements, economic volatility, environmental changes, and geopolitical shifts, the need for effective risk management requires no emphasis. From economic uncertainties to cybersecurity threats, supply chain disruptions to regulatory compliance, every organization faces an uncertain future. Effective risk management means proactively identifying, assessing, and treating potential risks that are likely to impede achievement of organizational objectives.

I recognize the fact that risk management is a very challenging discipline because risks lie in the future, and the only thing we are certain about the future is uncertainty. However, there is no reason to worry, The Risk Echo magazine provides a wide range of articles entirely focusing on risk and risk management. Different authors with varied experience and expertise in risk management explain the concept of risk and risk management and provide practical ways of managing risk. Whether you are an experienced risk professional seeking fresh perspectives or a new person to the concept of risk management, this publication aims to provide valuable insights that will enhance your understanding of risk management and decision–making capabilities. I encourage you to delve into the pages ahead, ponder over the issues and ideas presented and apply the concepts to your own unique context. I hope this publication will serve as a catalyst for change, enabling you to build resilience, seize opportunities, and thrive amidst uncertainty.

Finally, I would like to express my gratitude to the authors who have generously shared their expertise and experiences. Their collective wisdom and dedication have helped shape this publication into a valuable resource for risk practitioners, executives, policymakers, and anyone seeking to navigate the unchartered waters of today's world.

Edward Senyonjo
Chief Risk Officer,
National Social Security Fund

TABLE OF CONTENTS


AI

RISK
MANAGEMENT

PENSION

Q&A

WITH GEOFFREY W. SAJJABI, THE CHIEF COMMERCIAL OFFICER AT THE NSSF

QN: Mr. Geoffrey Sajjabi, thank you for accepting our interview. Kindly tell our readers who Geoffrey Sajjabi is and your role at the National Social Security Fund (NSSF).

First, I am a husband and a father. Born in Mayuge district, I consider myself part of the last generation to be raised by an entire village. My father was a Superintendent of Police and Prisons, and my mother, a housewife and a farmer. Right from a young age, our parents instilled in us the values of hard work and integrity, values that have guided my life and career. I started my education in rural Mayuge and later moved to Kiira College Butiki in Jinja for both O' and A' level education, before joining Makerere University, where I graduated in 2008 with a Bachelor of Arts degree. I hold a Master of Business Administration from Heriot–Watt University UK. I am also a holder of leadership and management certificates from Gordon Institute of Business Science, University of Pretoria, as well as Strathmore Business School, Nairobi. I am an alumnus of the Administrative Officers Law course of the Law Development Centre Uganda.

I am the Chief Commercial Officer at the NSSF, responsible for business growth and member retention, through improving compliance and expanding membership. I am also responsible for improving member experience through enhancement of processes, such as benefits payment, data management, and extension of financial literacy to enable members make sound financial and investment decisions. Given the recent amendments to the NSSF Act, I am now tasked with increasing social security coverage and contribute to better retirement outcomes for members of the scheme.

QN: How does that role contribute to the Fund's vision of being a social security provider of choice?

Driving compliance of contributing employers ensures that members of the Fund are guaranteed a decent retirement, and this should be motivating enough for people to embrace saving with NSSF.

We have also rolled out a financial literacy programme for members to enable them to make better financial and investment decisions.

Furthermore, by reducing turnaround time for payment of benefits, from an average of more than 30 days a couple of years ago, to about 10 days currently, and with a strategic target of 1 day by 2025, I have no doubt that we are positioning the Fund to be the social security provider of choice.

QN: What are the key challenges you face in this role and how do you address them?

Our biggest challenge relates to compliance. Thousands of entities struggle to comply with their social security obligations. Many employers have accumulated significant amounts of arrears, something that poses a challenge of recovery. We are dealing with employers whose cash flows are highly constrained. Data quality has also been a challenge for long, especially, given that since independence we have not had a national database that maintains up to date citizens registration information. Poor quality data affects decision making and ultimately impacts turnaround time on payment of benefits.

We have largely operated a relationship approach that brings employers and NSSF to a discussion. These discussions often result in long–term payment plans that are sensitive to the employers' cashflows. We have also often run amnesty campaigns to extend waiver of penalties to defaulting employers as one way of encouraging them to work towards gradual compliance. For instance, we extended waiver of penalty to over 1,700 employers during the Covid–19 crisis. Employers deferred payment of contributions without the risk of penalty.

The recent establishment of NIRA to deal with registration has been a game changer, despite its current challenges, we can only hope for better going forward. We now require new members to have registered with NIRA. This means that we no longer collect data which is already available within the NIRA database.

This requirement does not only improve data quality, but it also makes the registration processes convenient and faster. Members can register anytime anywhere. Although we still have challenges with individuals without NINs, we are optimistic that, this too, will soon be addressed.

QN: What is the eligibility criterion for membership in the NSSF?

Following the recent amendment of the NSSF Act, individuals employed with eligible employers are required to join NSSF as contributing members. Members are drawn from the age bracket of 16–55 years, although one can continue to voluntarily save beyond 55 years of age. The key determinant therefore, is that, one is working with an eligible employer, regardless of the number of employees.

The NSSF Act, as amended, has defined an Employer under Section 1(d), to include the following.

- The government of Uganda.
- Company registered or incorporated under the Companies Act, 2012.
- Partnership registered under the Partnership Act of 2010.
- Trustee incorporated under the Trustees Incorporation Act, Cap. 165.
- Business registered under any other law for the time being in force governing the establishment of business entities.
- The governing body of an unincorporated association; and
- Manager or a subcontractor who provides employees for the principal contractor.

In addition, members can now join the voluntary scheme and begin to save with the Fund. All people employed in the informal sector and those self–employed can now opt to join voluntarily. So, in short, all Ugandans can choose to voluntarily save with the Fund, including those under other existing mandatory schemes like Public Service or Parliamentary Pension scheme.

Existing mandatory contributors can also choose to make additional contributions over and above the statutory 5% monthly contribution.

QN: I understand you register both employees and employers for purposes of contribution. How often are they supposed to remit contributions and how much?

Employers are required to remit contributions monthly. The standard of the law is that contributions of the current month should be paid by the 15th day following the month for which relevant wages have been paid.

For example, the contributions relating to salaries of June 2023 ought to be paid by 15th July 2023. The law does not provide for amounts but rather percentages. Employers are required to deduct 5% from the employee's gross salary and top it up with 10% of the employee's gross salary, making it 15% per month.

For voluntary contributors, the law is flexible. These can choose to pay daily, weekly, monthly, annually or at any such intervals that might be convenient for the voluntary members.

We are still in the process of coming up with regulations for voluntary contributions and benefits, and these will, among other things define the amount.

QN: **What does it mean for an employer to be NSSF compliant?**

An employer is considered compliant when they meet the following:

- Payment of the right amount based on an employee's gross salary.
- Payment for all eligible employees.
- Payment on the right date, i.e, the 15th day following the month for which the relevant wages were paid.

QN: **What should I do if my employer refuses to remit contributions to the NSSF?**

We have a whistleblower platform where members and the public can report non–compliant employers. This can be accessed via the Fund website. Members can also report to our branches or contact their relationship managers.

QN: **What kind of benefits does one get as a result of being a member of the NSSF?**

The NSSF Act Cap 222 (as amended) provides for the following benefits:

- Age benefit, payable to members upon attaining 55 years of age or to members who are 50 years of age but out of gainful employment.
- Withdrawal benefit, paid to members upon securing employment with exempted employers.
- Invalidity benefit, paid to members who are either permanently or partially incapacitated, and as a result are unable to continue working.
- Survivors benefit, payable to the immediate dependent relatives of a member who passes on before accessing their benefit.
- Emigration grant, paid to both Ugandans and non–Ugandans upon permanently exiting the country.
- Midterm benefit, payable to members who attain 45 years of age and have contributed for at least 10 years or persons with disabilities who have attained 40 years of age and have contributed for at least 10 years.

QN: **If a member dies when he has multiple wives and children, how do they share the money?**

The NSSF Act, which largely borrows from the Succession Act, spells out the distribution criteria, with percentages prescribed for different beneficiaries. The multiple spouses and children would therefore, share the benefit as per the distribution criteria specified in the law or as agreed upon by the legitimate beneficiaries at the time of making the application. We are also guided by Letters of administration or probate in the processing of survivors' benefits. Legitimate beneficiaries can decide to choose individual(s) to whom the funds can be paid.

QN: **The amended NSSF Act became operational on 7th January 2022, and one of the key amendments was the change of threshold from five employees to one. This was intended to increase social security coverage to more Ugandans. Since then, to what extent has this objective been achieved?**

The change of the threshold has seen a significant growth in the number of registered employers. From January 2022 when the law came into force to date, we have registered 4,148 employers with less than 5 employees, and these have contributed UGX 6.1billion.

For the period July 2022 to June 2023, the number registered is 2,691, contributing UGX 2.1billion. 45% of the total registered employers this financial year are within the category of those that employ less than 5 employees.

We have seen a growth of 65% in employer registration compared to the last financial year and this is largely driven by lowering of the threshold. The numbers, therefore, demonstrate that the removal of the 5–employee threshold is having a positive impact on the business.

QN: **The change of threshold from five employees to one, does it mean my maid at home or shamba boy is supposed to register and contribute?**

As explained above, the NSSF Act, as amended, defines an employer for the purpose of making mandatory contributions, and that definition does not include homesteads.

It would be practically hard to enforce compliance within people's homes if the law was to define homesteads as employers. However, the law does provide an opportunity for individuals to make voluntary contributions.
Therefore, domestic workers and all people that might be working for entities that are excluded from eligible employers, can choose to register and contribute voluntarily.

QN: **Another key amendment was giving the board authority to innovate and develop additional products. Which new products have you developed so far?**

We are at an advanced stage of developing regulations for voluntary contributions and benefits. These will define the benefits that will be available to voluntary savers, and these will incorporate aspects of flexibility in terms of access to benefits, different from the mandatory contributions. We are, however, not at liberty to discuss these options until the Minister responsible for social security issues the relevant regulations.

We have also started discussions around the possibility of introducing additional benefits for the mandatory savers and we might partner with other players to actualize this. Of course, the critical thing to establish is whether any additional benefit would meet the sustainability test.
We will have to undertake studies on the likely impact of any proposals on the scheme's long–term sustainability.

QN: **If I am not required by law to register with the NSSF, can I join voluntarily, and when do I get my money?**

Yes, any member of the public who is not covered under the mandatory category can choose to join and contribute voluntarily. Even those already saving under mandatory category, can choose to make additional voluntary contributions, over and above the statutory 5%.
We have developed a range of options that will enable the voluntary saver to determine the duration for which they want to save, and these options have inbuilt flexibility in terms of access to benefits. Once the Minister issues regulations, we will undertake mass public sensitization regarding the new options for voluntary members.

QN: **What do you tell people who are concerned about the safety of their money in the NSSF?**

We have robust and transparent systems in place to ensure safety of member funds. We are guided by high ethical and professional standards in execution of our duties, and we are committed to the interests of the member.

Our performance over the past 10 years has also demonstrated that we create value for members by undertaking prudent investments that largely emphasize safety.

Our performance and systems are also subject to external scrutiny by the Auditor General. We are regulated by the Uganda Retirement Benefits Regulatory Authority in addition to the oversight by the respective Government Ministries.

We also have a tripartite Board, representing members, employers, and the Government, which ensures that our decisions are informed by interests of the members.

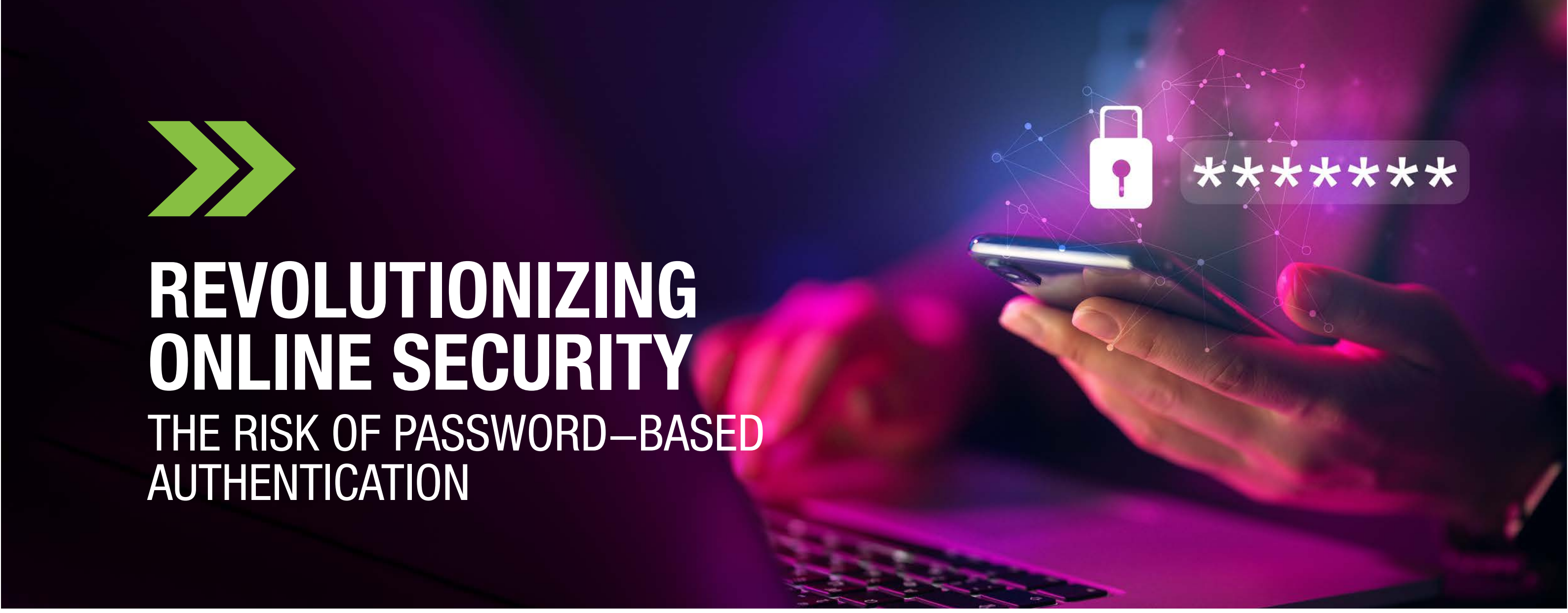
These governance systems and accountability mechanisms should give our members reasonable assurance regarding the safety of their funds. The ultimate test is that, when you become eligible to access your money, it is available; this is something that we have consistently done.

QN: Anything else you would like to tell our readers concerning the NSSF?

All of us will become old at some point in time, and we will not be in active employment forever. We must, therefore, prepare for that time when we still have the means and energy.

It is important to note that, with the current life expectancy in Uganda of 64 years, we are likely to live longer than our forefathers. This calls for more savings and investments to mitigate old age poverty and misery.

Let us embrace all opportunities to save and invest now. Our children will not look after us, let us plan with a mindset that we are likely to continue supporting our adult children long into our retirement. This calls for action now. Save and invest when you still can.



REVOLUTIONIZING ONLINE SECURITY

THE RISK OF PASSWORD–BASED AUTHENTICATION

Hope Victory Shaba
Information Security Specialist,
National Social Security Fund

Remembering passwords can be a hassle. We've all been there; you're trying to log in to an account and you can't remember the password. You try a few different combinations, but nothing seems to work! Maybe you're using the wrong email address, or you've forgotten which special characters you used, or you're just plain forgetful. Whatever the case, it's frustrating. But what if there was a way to log in without having to remember a password at all?

In the world of digital security, passwords have long been the gatekeepers of our online experience. We've all heard the advice: use strong passwords, don't reuse them across multiple accounts, and change them frequently. Let's be real, how many of us actually follow those guidelines? And even if we do, passwords are far from foolproof. With data breaches and hacking attempts becoming more and more common, it's clear that we need a better solution.

Passwordless authentication is the new kid on the security block that promises to make logging in simpler, faster, and more secure than ever before. But is it really the future of digital security, or just another passing trend?

In this article, I'll dive into the world of passwords and passwordless authentication, exploring the pros and cons of each and helping you decide which approach is right for you. So, buckle up, because we're about to take a deep dive into the world of digital security!

The problem with passwords

Passwords have been around since the early days of computing, and they remain the most used form of authentication. However, passwords have significant drawbacks that have become increasingly problematic as technology advances.

i) Memorization

One major problem with passwords is that they're easily forgotten. In fact, Forrester Research estimated that between 20% and 50% of all helpdesk calls are related to forgotten passwords. Additionally, passwords can be easily guessed, stolen, or cracked, especially if they're not strong enough. This makes them a weak point in security systems.

ii) Duplication across multiple accounts

Another issue with passwords is that they're often reused across multiple accounts, making them even more vulnerable to attack. If a hacker gains access to one account with a weak password, he/she may be able to access other accounts using the same password.

To address these issues, many organizations are turning to passwordless authentication as a secure and user–friendly alternative.

What is Passwordless authentication?

Passwordless authentication is a method of authentication that does not require users to enter a password to access their accounts. Instead, it relies on other forms of authentication, such as biometrics, security keys, or one–time codes.

Passwordless authentication, the new buzzword in the world of digital security, is a game–changing technology that promises to revolutionize how we access our online accounts. Gone are the days of trying to remember complicated passwords or jotting them down on scraps of paper. With passwordless authentication, you can log–in to your accounts in a snap without ever having to type in a password again!

Passwordless authentication isn't just about convenience but also offers a level of security that traditional passwords simply can't match. By eliminating the need for passwords, passwordless authentication eliminates the risk of password–related attacks like phishing, keylogging, and brute force attacks. With biometric factors like fingerprint or facial recognition, passwordless authentication ensures that only you can access your accounts.

So, whether you're tired of trying to remember yet another password or concerned about the security of your online accounts, passwordless authentication is the answer you've been looking for. With its unbeatable combination of convenience and security, it's no wonder that passwordless authentication is quickly becoming the future of digital security!

Why passwordless authentication such a big deal

For starters, it's more secure than traditional password–based authentication. Passwords can be easily guessed or stolen, and even if you use a strong and complex password, it can still be compromised in a data breach. With passwordless authentication, there's nothing to steal or guess. You're relying on a physical attribute or a unique code, which makes it much harder for an attacker to gain access to your account.

Another benefit of passwordless authentication is convenience. It's much easier to scan your face or use your fingerprint than it is to remember a complicated password. And if you're using a mobile device, you don't even need to type anything in. Just a quick tap or scan, and you're logged in.

Perhaps the biggest benefit of passwordless authentication is that it can help reduce the number of support requests related to forgotten passwords. As mentioned above, according to a study by Forrester Research, password–related issues account for 20% to 50% of all IT helpdesk requests. That's a lot of time and resources wasted on something as simple as forgotten passwords. With passwordless authentication, those requests go away.

How passwordless authentication works

Instead of relying on traditional passwords, passwordless authentication uses a variety of cutting–edge technologies to verify your identity. These include biometric factors like fingerprint or facial recognition, hardware security keys, or even behavioral analytics that analyze how you interact with your device. The passwordless authentication technology comes in three ways, each with its pros and cons as explained below:

i) Biometric authentication

Biometric authentication uses a physical attribute like a fingerprint or facial scan to verify your identity. This method is highly secure, as it's difficult to fake a fingerprint or facial scan. However, it does require a compatible device, and there are privacy concerns associated with storing biometric data.

ii) Push authentication

Push authentication is where you receive a notification on your phone or other device that asks you to approve or deny a login request. This method is also highly secure, as it requires physical access to your device to approve the request. However, it can be less convenient, as you must always have your device with you.

iii) Email or text–based authentication

Email/text–based authentication, is where you receive a one–time code via email or text message that you use to log in. This method is less secure than biometric or push authentication, as it's easier for an attacker to intercept the code. However, it's still more secure than a traditional password, and it's highly convenient.

Additionally, it is important to note that no security control is foolproof, even biometrics such as fingerprints can be cloned. For instance, if you touch an object, your fingerprints stay on that object for some time and they can be pick and used anywhere, including accessing your account.

Therefore, the strongest authentication control measure would be a combination of the different authentication methods.

The future of digital authentication

More and more companies are adopting passwordless authentication as a way of improving security and reducing support requests. As technology continues to evolve, we can expect to see even more innovative methods of passwordless authentication.

Of course, there are still some concerns to be addressed. For example, biometric data must be stored securely and protected from hackers. And there's always the risk that a device could be lost or stolen, compromising the security of a passwordless authentication system. But overall, the benefits of passwordless authentication far outweigh the drawbacks.

CONCLUSION

Passwordless authentication is not just a buzzword for IT experts – it's a revolutionary concept that has the potential to transform the way we access and secure our digital identities. As an IT security practitioner, I've seen firsthand the problems that traditional passwords can cause, from forgotten login information to data breaches and cyber–attacks. But with passwordless authentication, we can say goodbye to these problems and welcome a new era of convenience and security.

THE CHANGING RISK LANDSCAPE IN THE FINANCIAL SECTOR

Kayizzi Ronald Musoke
Senior Middle Officer,
Bank of Africa BMCE Group

Risk, as defined by the COSO (Committee of Sponsoring Organizations of the Treadway Commission), is the possibility that events will occur and affect the achievement of strategy and business objectives. In the context of investment, risk refers to the uncertainty and potential for financial loss associated with an investment's performance. It has been said that not taking a risk is the biggest of all risks (Facebook CEO Mark Zuckerberg).

Investments inherently involve risk because their returns are uncertain and can fluctuate. Various factors contribute to investment risk, including market conditions, company–specific risks, and other external events.

Investors assess and manage risk by considering their investment objectives, time horizon, risk tolerance, and diversification strategies. Diversification, for example, involves spreading investments across different uncorrelated asset classes, sectors, or geographic regions to reduce the impact of a single investment's poor performance.

As investors utilize risk assessment tools such as risk fishbone diagram, risk ratings, what if analysis, decision tree, delphi technique, etc to evaluate and mitigate risks, they need to put into consideration emerging risks. Below are some of the emerging risks within the financial sector:

Cyber risk

Rapid advancements in technology, such as artificial intelligence, blockchain and crypto–currencies, and other fintech innovations, increase the attack surface. According to data released by Interpol Uganda in October 2021, Ugandan banks lost over $4 million to hackers in one year. The Director of Interpol at the time said the theft was carried out via technology and involved bank fraud, fake visa issuance and online business.

Every cybercriminal would want to target banks because this is where the money is. Therefore, banks need to prioritize cyber security, by keeping pace with developments in cyberspace, building a robust security infrastructure, having a 24/7–monitoring capability of their systems, and conducting vulnerability assessments and penetration testing regularly.

Regulatory compliance risk

Evolving regulatory regimes give rise to new risks. Changes in financial regulations or shifts in regulatory priorities can impact the risk landscape.
The proposed increase in minimum capital requirement from UGX 25bn to UGX 150bn by the Central Bank of Uganda in 2022, is a significant risk to several banks. As of 31/12/2022, only 45% of the banks had capital equal to or above the proposed limit of UGX150bn, according to the 2022 audited financial statements of the banks. The banks have up to June 2024 to comply with this requirement.

The banks should use the grace period to build adequate capital, such that, come June 2024, they are able to comply with the capital requirement. Alternatively, smaller banks that cannot meet this requirement, may consider a merger.

The Data Protection and Privacy Act provides severe penalties (2% of annual revenue) for breach of personal data; that cost excludes legal fees and compensation to the victims.

To mitigate the risk of penalties and the associated costs, banks need to develop robust data protection frameworks and infrastructure and conduct regular awareness training for their employees.

Competition from non–traditional financial institutions.

It is increasingly becoming common to find non–financial institutions, such as telecom companies offering financial services, that have for a long time been a domain of the financial institutions. Telcom companies now accept deposits and make cash payment (Mobile money), they also extend credit in terms of airtime to their clients, which can be used to purchase internet bundles. The growth of mobile money (MM) has been phenomenal. Below are some statistics on the growth trend of mobile money for the last three years.

Year	Number of MM active accounts	Total value of MM transactions
2020	UGX 24.1 million	UGX 10.4 trillion
2021	UGX 26.7 million	UGX 12.9 trillion
2022	UGX 29.3 million	UGX 15.4 trillion

These transactions would have potentially been in the banking sector. To counter this risk, banks need to be more innovative, especially in the fintech space.

Interest rate risk

Interest rate risk is the potential loss arising from changes in interest rate. A significant portion of commercial banks' assets are government securities (Treasury bonds and bills). On average, the ratio of treasury assets to total assets was 15.2% in 2021 (Bank of Uganda Financial stability report June 2021).

However, of recent, the Ministry of Finance, Planning and Economic Development has indicated that the government is weary of domestic borrowing, which is characterized by high interest rate. The risk is that when the government reduces domestic borrowing (supply of securities), the price (demand for securities) of the securities will increase, due to the forces of demand and supply. Consequently, interest rate on securities will go down because of the inverse relationship between interest rate and price of government securities.

As a mitigation, the banks need to review their asset allocation, and undertake appropriate diversification.

Exchange rate risk

Foreign exchange rate risk or currency risk is the exposure to potential gains or losses due to changes in the value of one currency in relation to another. This can have a significant impact on Ugandan banks and other financial institutions, as they often have foreign currency–denominated assets and liabilities.

To manage this risk, financial institutions can use a variety of hedging techniques, such as forward contracts, futures contracts, and options. These techniques can help to protect banks from losses caused by changes in exchange rates. However, hedging techniques can be expensive, and they may not always be effective. In some cases, exchange rate movements can be so large that even hedging techniques cannot protect banks from losses.

Inflation risk

Inflation, the general increase in prices over time, undermines the performance of an investment, the value of an asset, or the purchasing power of a stream of income. Fixed rate bonds are most at inflationary risk because their payouts are generally based on fixed interest rates, meaning an increase in inflation diminishes their value.

Financial institutions can take a number of steps to mitigate the risk of inflation, such as: Investing in assets that are likely to appreciate in value during periods of inflation, such as real estate and commodities, hedging against inflation by using financial instruments such as inflation–linked bonds and derivatives, managing their costs carefully to ensure that they are not overly exposed to inflation, as well as building up reserves to cushion against losses caused by inflation.

Fraud risk

The risk of fraud in the financial sector is always considered high. However, in hard economic times, such as during and post–Covid–19 periods, coupled with the effects of the war between Russia and Ukraine, which disrupted global supply chains, leading to unprecedented high inflation globally, the risk of fraud is higher than ever before. According to the Uganda police force, reported fraud incidents increased by 25% during/post–Covid–19 period compared to the pre–Covid–19 period. This mainly resulted from increase in on–line transactions as opposed to face–to–face transactions.

The banks and other financial institutions need to regularly conduct fraud risk assessment and evaluate the strength of their controls in mitigating the risk of fraud. Identified gaps should be immediately addressed.

Secondly, the banks need to increase fraud information sharing; fraudsters have a tendency of trying out their practices in various banks.

Thirdly, banks need to enhance their KYC procedures to curtail any form of impersonation.

Changing customer expectations

Customer expectations are constantly changing, and businesses need to be prepared to adapt. Customers are more likely to switch to a competitor if they are not satisfied with the product or service they are receiving.
Customers who are unhappy with a product or service are more likely to share their negative experiences online, which can damage a company's reputation. Businesses need to collect customer feedback and use it to improve their products and services to create better experiences for customers. Businesses need to be socially responsible (Give back to the communities in which they operate). This will help to build goodwill and support from customers.

CONCLUSION

The aftereffects of Covid–19, coupled with the effects of the climate change, geopolitical tensions, and regulatory changes, have raised the risk landscape in the economy and more specifically in the financial sector. Business leaders in the sector need to keep their eyes on the horizon to be able to figure out the emerging risks to their businesses and proactively address them.

BANK OF AFRICA
BMCE GROUP

BANK OF AFRICA ENHANCED DIGITAL PAYMENT SOLUTION

With a large portfolio of diversified financial solutions, BANK OF AFRICA – UGANDA Ltd. enhanced it's Mobile Wallet bouquet and added BOA Pay to further increase payment convenience.

BANK OF AFRICA – UGANDA Ltd. (BOA) added **BOA Pay** to its Mobile Wallet menu in June 2022 in a bid to increase payment convenience. BOA Pay is a payment solution that allows the Bank's customers to pay for goods and services at partner merchant locations. The digital payment service is enabled for the Mobile Wallet application and USSD on ***246*7#**.

The payment solution aims at promoting cashless transactions, easing payments for customers, and enabling a seamless customer experience at zero cost to the merchant and the customer.

Why a payment solution?

The Bank's strategic formula is grounded on enhancing the customer's experience through the implementation of new digital technologies. The COVID-19 pandemic was an undeniable catalyst for change and accelerated digital transactional activity in the country.

With our understanding of consumer payment preferences, the Bank enhanced its digital offering with BOA Pay, a secure, seamless and convenient payment option for our customers.

We believe in creating innovative, efficient and effective digital solutions for consumers and businesses of all sizes. BOA Pay is one of the innovations that reinforces our commitment and we look forward to our customers benefitting from it.

What is unique about the service?

The BOA Pay is an intermediary solution between the bank, a person or organisation that needs to receive funds, and the person or organization seeking to purchase goods or services.

The merchants enrolled on the BOA Pay platform are in several categories such as hospitality, dining, consumer goods store, health (hospitals, pharmacies), and fuel stations among others. We believe these merchants will be able to serve our customers.

What are the BOA Pay charges?

We are actively promoting cashless transactions therefore, BOA Pay is free of charge for both the merchant and customer.

How have consumers facilitated growth in digital payments?

Digital payment transactions have grown rapidly in emerging markets during the past two years as the pandemic accelerated shifts to contactless and e-commerce payments.

It is therefore imperative for a business that transacts with consumers to widen its assortment of digital payment options.

Consumers are driving multiple payment options as they seek easy, convenient and quick solutions. Consequently, it is upon businesses like BOA to provide alternative innovations such as BOA Pay which are frictionless solutions to both consumer and merchant needs.

We launched BOA Pay with one merchant and only 4 outlets, we currently have over 117 merchants with 125 outlets across the country. We intend to recruit more merchants in several sectors and categories that will extend services to all BOA customers and eventually the non-banked mobile money telecom user.

What should customers expect?

The Bank is continuously investing in the enhancement of its channels to facilitate customer interactions and provide a superior customer experience.

With the constantly changing customer needs, we have improved the ways customers interact with us, so whether it is online account opening, transactions at banking centres, or digital channels, we have huge milestones with several choices.

BOA Pay is currently available at over 125 outlets countrywide. We will continue to recruit and on board merchants for the service. BOA Pay signage is displayed at the respective outlets where BOA Pay payments are acceptable.

What are the benefits of BOA Pay?

There are multiple benefits of BOA Pay for both the customer and merchant and these promote convenience and are ingredients for a business' growing needs.

For the customers;

- **Secure and cost-effective** as risks associated with cash handling are reduced
- **Customer convenience**
- **Free transactions**
- **Enhances accountability**

For the merchant;

- **Secure and cost-effective** as it reduces overhead costs and risks associated with cash handling
- **Customer convenience and satisfaction**
- **Enhances accountability and maintains an audit trail**

How to use BOA Pay

The BOA Pay provides customers with two payment options, using the Mobile Wallet by scanning a QR code, or using the USSD text messaging service on *246*7#.

How to become a merchant

If you are a registered entity, visit the nearest BOA Branch or visit the website https://boauganda.com/

Tel: 0414 302 001 | **Toll-free:** 0800 100 140 | 0776 400 601 | **Email:** feedback@boauganda.com | **Web:** www.boauganda.com

BANK OF AFRICA - UGANDA Ltd. is regulated by Bank of Uganda. Customer deposits are protected by the Deposit Protection Fund up to UGX 10million, Terms and Conditions apply.

QUIET QUITTING:
A SALIENT ORGANIZATIONAL KILLER.

Okutre Jesse
Operational Risk Specialist,
National Social Security Fund

When Covid–19 forced people to work from home, it increased the appetite for self–employment. Just after the world was declared free of the Covid–19 pandemic, as life was returning to normal, there was a great resignation, where 71.6 million people in the USA alone separated from their jobs between April 2021 and April 2022, according to the US Bureau of Labor Statistics. This averages 3.98 million people quitting monthly and by June 2022, the number of people quitting had reached 4.2 million monthly.

The great resignation was driven by the fact that the employed population had gotten used to working from home and preferred a limited workload and flexibility in working from home. Even among those who have continued in employment, some exhibit what is commonly known as "quiet quitting."

Quiet quitting doesn't refer to resignation or quitting a job; it means completing one's minimum work requirements without going over and above what is required, that is, the employee decides to work as per the bare minimum (no more time, effort, or enthusiasm than required). Such an employee's main objective is to pick their salary or wages at the end of the month. Some other signs could include; not attending team meetings, arriving late or leaving work early, reduced productivity, little contribution during team meetings, and lacking passion for the job.

The word quiet quitting may be trending now, although it is not new. This practice has been around for some time. But what could be the causes of employees quitting quietly?

Excess workload

Quiet quitters are individuals who were once hard–working employees, but because of the work overload, they tend to suffer from burnout and become less engaged, taking work for granted. Burnout could result from competition among employees or working long hours trying to achieve stringent targets.

Change in individual priorities.

According to the talent trends 2022 report, during the pandemic, people had time to think, question their careers, and seek more work–life balance. People took to social media to promote their discontent with work, and others resorted to self–employment by becoming content creators on social media. Therefore, Covid–19 became a new driver of quiet quitting.

Poor Compensation

Poor compensation is a leading cause of quiet quitting. Quiet quitters usually feel they are doing too much work for too little pay. The moment an employee feels improperly rewarded for their effort, chances are, they will scale down.
When the employer shows less appreciation for the sacrifice and effort of the employees, they will feel taken advantage of and withdraw their commitment and effort.

Lack of proper work–life balance

Quiet quitting is sometimes a reaction to poor work–life balance and a disregard for work and personal life boundaries. When the employer does not draw a line between when one is at work and home, and keeps calling and sending emails even after work, such acts make employees feel that the company does not respect and protect their personal time.

Unsupportive managers

Whenever employees feel that they don't get the necessary support or help from their leaders, they build invisible barriers around themselves, thus withdrawing from the rest of the group. Generally, employees are often able and willing to work through challenging conditions when they know they are backed by the leaders who are caring and considerate. These acts of kindness keep the employee motivated.

However, should leaders/managers fail to show any signs of caring, being considerate, or advocating for their employees, the employees are more likely to quit quietly when they feel their managers/leaders don't have their best interests in mind.

Poor communication or lack of conflict–resolution skills

Sometimes, quiet quitting comes because of poor communication. Let's take an example of dismissing a co–worker as stupid or an idiot for presenting a plan that needs improvement or calling your employees lazy rather than focusing on specific impediments to better their productivity. This type of response can make a person withdraw from the group. It worsens if one does not know how to resolve conflicts; the employee may be afraid of conflict and never raises the issue, quietly pulling back instead of informing their bosses.

Before we dig into how these can be prevented or avoided, let's look at the impact of quiet quitting:

i) Decrease in organizational performance

The chemistry is working as a team, which increases organizational performance. However, a quiet quitter prefers to work in isolation. Quiet quitters never contribute to team cohesion, discussions, brainstorming sessions, and building a positive organizational culture, which consequently affects the organizational output.

ii) Inter–team conflict.

Quiet quitters are individuals that have a lazy attitude and tend to be aloof and only prioritize their interests. This kind of attitude may not go well with other workmates, and the lazy attitude will eventually spill over to the teammates in terms of excess tasks carried on by those still interested in the job. This kind of attitude can cause divisions among teams; a problem with one employee may quickly become a problem for all employees. These conditions can lead to passive–aggressiveness or conflict within the team, and neither outcome is ideal, since trust and dependability are essential for teamwork.

iii) Low workplace morale

One employee's low morale can spread and affect the team's attitude and performance. Like yawning, a bad attitude is contagious, and a distressed or apathetic employee can take a toll on peers, especially if the colleagues are highly empathetic. If not dealt with immediately, quiet quitters can be detrimental to the entire team (one rotten apple spoils the whole barrel).

The good news is that quiet quitting can be cured in the following ways:

a) Create psychological safety

One of the most effective ways to address quiet quitting is to have an open and honest conversation with employees. You can take the "quiet" out of the quiet quitter by airing the issues in the open. For example, employees should feel comfortable enough to have open and honest discussions, and you (as a leader) should clarify that this conversation is not punishable.

Employees should feel safe when they speak in the presence of their leaders or managers. The moment more talking is done in the absence of the managers after a formal gathering, then know the employees do not feel safe, thus increasing the chances of quiet quitting.

b) Employee surveys and feedback

The entity can create platforms where honest feedback can be picked from the employees. For example, NSSF conducts annual employee surveys where feedback is anonymously given through a series of questions. Management then investigates and resolves the identified issues. This practice allows employees to express their opinions without fear or favour.

c) Hold the end of the bargain up

Walking the talk shows employees that management is true to their word, and are serious, sincere, and supportive. This simple act can go a long way in restoring the employee's faith and work ethic. Follow–through is always critical when dealing with quiet quitters; unfulfilled promises and lip service may worsen the disengagement problem.

d) Performance reviews

This is a powerful tool in fighting quiet quitting, where managers review the performance of their employees. This creates and encourages ongoing open dialogue with employees, where managers get to hear from their employees about current projects they're working on, the obstacles they face, and what kind of support and resources they need to succeed.

Though performance reviews are a powerful tool, the frequency of the reviews needs to be considered; weekly reviews can seem like micro–management. The reviews could be quarterly or bi–annual.

The meeting outcomes should be a road map to help guide employees toward the growth they want in their career path. Secondly, the employees should walk away from the meetings with a clear understanding that their abilities and potential are recognized and appreciated.

Reward and recognition

If there is anyone that never wants recognition and rewards for the tasks performed, then that person is not from this universe. Employees want to be appreciated and feel valued for what they do. By recognizing and rewarding employees for good performances, you show the team that effort is appreciated and that what they do matters to the organization. Reward and recognition create a positive vibe in the work culture that gets quiet quitters out of their quietness.

Maintain boundaries and respect work–life balance.

Burnouts are common among employees, and this comes as a result of failure to balance professional and personal lives. Having a healthier work–life balance is possible even when some pressure is exerted on the employees. For example, emphasizing that answering after–hours calls or emails is optional, defining what constitutes a true after–hours emergency and then sticking to it, allowing employees who stay late to leave early the following day, etc. Whereas it is imperative to get the best out of the employees and employees giving their best to the organization, it is not advised to drive one towards the point of burnout.

CONCLUSION

Quiet quitting can be more detrimental than complete disengagement because it does not only lead to financial loss due to paying salaries for little or no work done, but it also breaks team cohesion, consequently affecting organizational performance. Managers or leaders must be able to identify early warning signals of quiet quitting and take proactive steps to address such negative behaviours before they become a serious problem

SOCIAL MEDIA AND PUBLIC RELATIONS MANAGEMENT: EVERY ORGANIZATION IS ONE TWEET AWAY FROM A DISASTER

Brian B. Mukalazi
Chief Executive officer,
Talis Consults Ltd

There are many laws of nature and one of them is that your greatest source of advantage is your greatest source of danger. This is true of social media; the greatest benefit of social media is its speed and ability to reach far and beyond within a very short time.

Many businesses that have embraced social media have created a competitive edge over those that have not taken full advantage of social media. However, social media is a double–edged sword, it can promote and grow your business rapidly, but it can also ruin your business within a matter of minutes!

About a month or so ago, one of my old clients, in a health institution, I will call XY hospital (not real name), faced the wrath of social media. This was after one of their former employees, a medical officer, Dr. P (not real name), took to Twitter to express his grievances with the hospital.

In a lengthy Twitter thread, Dr. P spoke of his despair at the hands of his former employer. In part, the tweets read: “July/1st/22, I was recruited to work as a medical doctor at XY Hospital on a full–time contract, running 16 duties a month paying a sum of Shs2.3m monthly, this money was only paid (July & August 2022) after having initially been part–time from May 2022 [sic]”. He added, “Dry spell hit when there was no money being paid…from September to December 2022 even with constant engagements with both the clinic head & the CEO………….”

He further tweeted that, in January 2023, having failed to recover his money from his employer, which had accumulated to Shs9.2m, he engaged a lawyer. The lawyer wrote a demand letter to the hospital with intention to sue if the employer did not pay the money in a specified period. Upon receipt of the letter, the Chief Executive Officer apparently panicked and requested for negotiations, which Dr. P was not willing to engage in. Eventually the hospital sent Dr. P Shs4m.

The tweets went on and on; in which he indicated that he decided to share because he saw so many doctors in private facilities being taken for a ride and not being paid, and that it was a shame that his fellow doctors were so much behind his predicament.

As you can imagine, the tweets went viral in just a couple of minutes, attracting attention from different Ugandans, including common folks, medical practitioners, Members of Parliament, activists, and government officials.

After what seemed like a long silence, the hospital issued a statement, and it was obvious that they were in a crisis mode. The statement was far from convincing, as it was short of humility and was devoid of clear acknowledgment of fault or error on their part. Inevitably, it generated more flurry from the angry public.

Dr. P could have been wrong, but at that moment, it didn’t matter. The damage was done! Risk incidents like this are on the rise today in the face of increased social media use. Social media is now considered by many as a more effective communication platform than the rest, and this presents completely new challenges for organizations and leaders.

While social media comes with multiple benefits, it can also be used as an instrument of blackmail, revenge, and spite. I have seen how easy it is for relationships (corporate or personal) to slip from a healthy status to disaster and some organizations have paid the ultimate price.

It is, therefore, important for leaders to be both purposeful and intentional with social media. There is need to strengthen public relations function, including development of solid, and executable crisis management plans to minimize damages that could be caused by social media.

To demonstrate this need further, here’s another social media incident and how it was managed.

On April 12, 2018, at a Starbucks Café in Philadelphia, USA, two African American men were waiting to meet a friend. When they asked to use the restroom, they were stopped because, apparently, they had not purchased anything. The manager subsequently asked them to leave.

When they refused, the police were called, and the two men were handcuffed, arrested, and removed from Starbucks. This incident was caught on video and went viral within minutes of being posted, sparking national outrage at what was seen as an ugly case of racial profiling and discrimination.

Just like in the case of XY Hospital highlighted above, Starbucks was besieged with anger and criticism.

Kevin Johnson, Starbucks' CEO at the time, suddenly found himself and his company thrust into a national controversy. But unlike the hospital CEO, Johnson took full responsibility. Here are several excerpts from his official statement made several days after the incident:

"I want to begin by offering a personal apology to the two gentlemen who were arrested in our store. What happened in the way that incident escalated, and the outcome, was nothing but reprehensible, and I'm sorry. I want to apologize to the community in Philadelphia, and to all my Starbucks partners. This is not who we are, and it's not who we're going to be. We are going to learn from this, and we will be better for it. These two gentlemen did not deserve what happened, and we are accountable. I am accounta

There were many ways Starbucks could have responded. The CEO could have blamed the Café employees, fired them, and simply stated that they weren't representatives of the spirit and culture of Starbucks. Or he could have blamed the Police for acting irrationally, but he chose to take full responsibility.

Kevin Johnson did more than just make a statement, he flew to Philadelphia and met personally with the two men to apologize to them and to make amends. Furthermore, he also knew that dealing with the root causes of this issue would require more than an apology.

So, first, Starbucks changed and clarified the relevant policy, and this was issued in a letter to all employees. In addition, he made an unprecedented commitment to conduct racial–bias training for all of Starbucks' 175,000 U.S employees.

No one knows what could have befallen Starbucks had the CEO acted otherwise. But one thing is known for sure, his meticulous, quick actions saved the day.

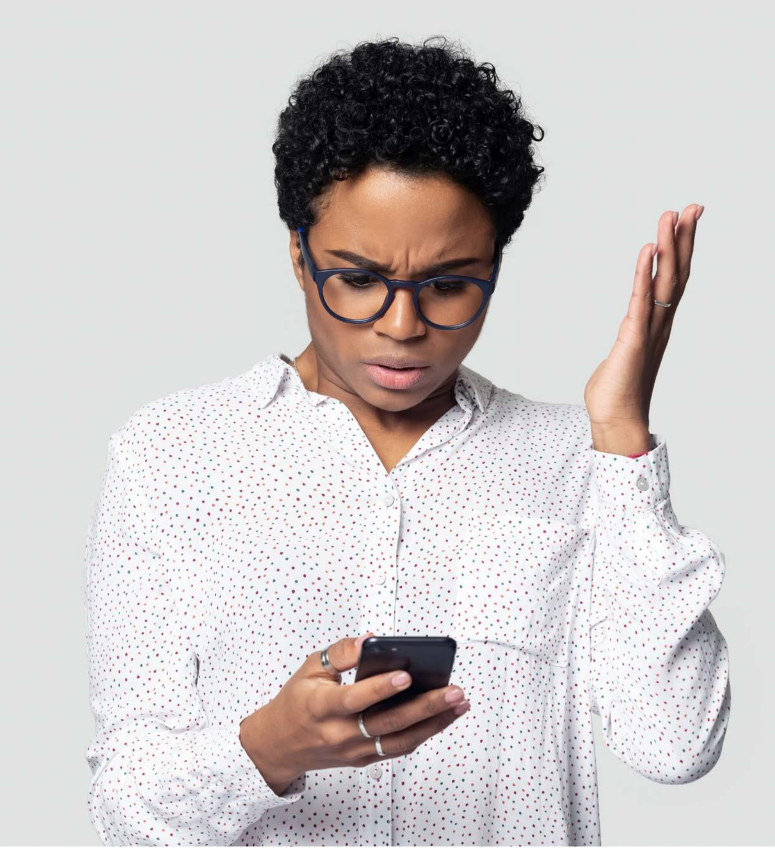
The sad truth is that organizations, no matter the size, will at different points make mistakes, which can all be candidates for potential social media criticism. It is, therefore, important that organizations develop social media management strategies.
Among other things, the social media management strategy should have guidelines on dealing with negative social media. I find the following tips from Forbes magazine (forbes.com, December 18, 2020), very useful:

i) Don't divert blame

Always take responsibility, even if you disagree with the author of the review. Take the negative feedback and respond respectively. Your strategy should be to take the conversation away from the public to the private domain; so, encourage the concerned party to call you or email you.

ii) Be respectful

Regardless of how negative the comments are or who has posted them, your response must be delivered in a respectful manner. Remember that any form of disrespect will generate more negative comments.



iii) Don't get defensive

Even when you know you are right, acknowledge comments. Be honest and explain the cause of the problem and how you are addressing it.

iv) Show that you are taking the matter seriously.

Comments on social media, regardless of how negative or outlandish they are, must be taken seriously. Responses must be carefully crafted to convey a sense of understanding as to why the comments were made.

V) Respond as quickly as you can

A speedy response shows the poster as well as others reading the comment that you care. It also allows you to shape the conversation before others potentially chime in and turn one post into a thread of negativity.

vi) Make sure the customer feels heard

When responding to criticism on social media, it's important to ensure that the customer feels legitimately heard. Acknowledge their frustrations, own up to the feedback they've shared, and encourage them to direct the message to you to make things right.

Conclusion

Here's my parting question to business leaders and other leaders: How prepared are you for the outcomes in case a social media disaster strikes?

Set yourself apart
market sp
t
C O

PSYCHOLOGICAL SAFETY:

A CRITICAL INGREDIENT FOR EFFECTIVE RISK MANAGEMENT

Sendiwala Micheal
Senior Investment Risk Manager,
National Social Security Fund

Psychological safety is a critical ingredient for creating a positive risk culture, lack of which may result in a toxic work environment.

According to Dr. Amy C. Edmondson, the scholar and Harvard Business School professor, psychological safety is a belief that one will not be punished or humiliated for speaking up, which she called a "felt permission for candor". Psychological safety is natured by an environment where;

Raising concern by any team member is acceptable, no matter the hierarchy.

If employees, regardless of their positions, are given an opportunity to make suggestions and raise issues of concern, this stimulates new ideas, which improve business processes and value addition.

The culture where a few employees have the privilege of being listened to, while others are marginalized, is a major barrier to psychological safety.

Ideas, right or wrong, are welcome, regardless of who is originating them.

Sometimes what appears to be a 'stupid' idea now, may turn out to be a game changer tomorrow. In 1903, Mr. Scott–Montague, an MP in the United Kingdom, said, "I do not believe the introduction of motorcars will ever affect the riding of horses". The idea of a motorcar at that time must have sounded stupid.

Another dismissal of a great idea came from Heinrich Dreser, head of Bayer's Pharmacological Institute, when he said, "This is typical Berlin hot air. The product is worthless." This was a comment in Dresser's letter rejecting Felix Hoffmann's invention of aspirin. Today more than 10 billion tablets of aspirin are swallowed annually. Furthermore, one of Chester Carlson's rejection letter about his invention of a Xerox machine he received in 1940 read in part, "Who the hell wants to copy a document on plain paper???!!!" According to Giji Van Wulfen's article, over 20 companies rejected Chester Carlson's 'useless' idea between 1939 and 1944. Even the National Inventors Council dismissed it. Today, the Rank Xerox Corporation has a market capitalization of $ 2.3bn.

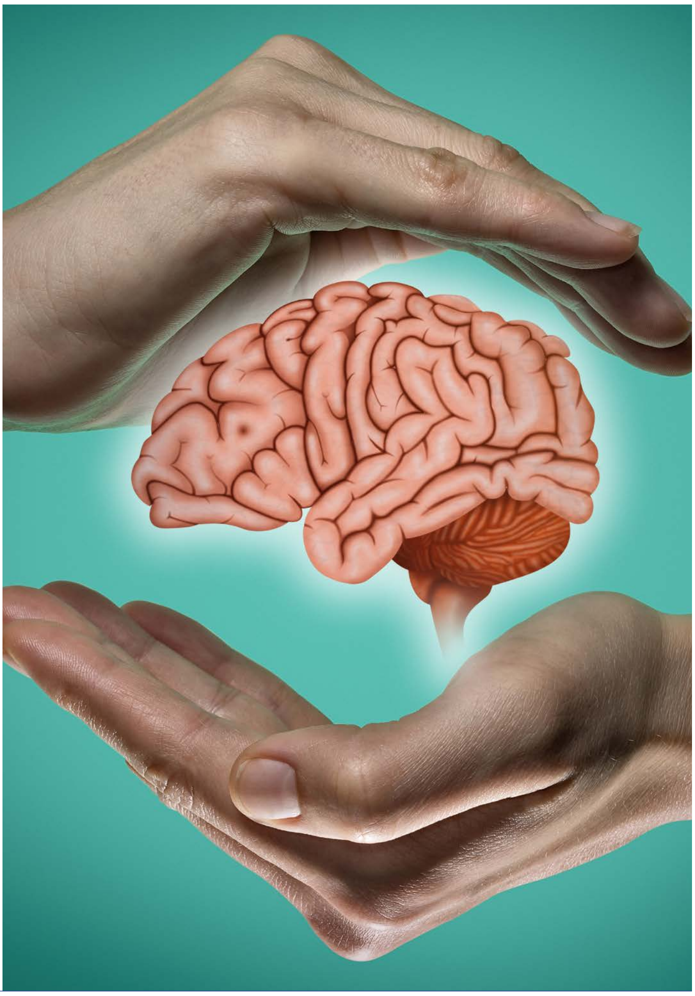
Open discussion and candid responses are encouraged.

An open environment is the birthplace of new ideas that can transform the organization. Unfortunately, oftentimes, work politics takes the day, where employees prefer to share information that pleases their superiors, while the latter focus on being praised, and often promote team members who glorify them (supervisors).

Consequently, several employees become cautious with the information they share. Otherwise, disseminating unpleasing information can be career–limiting. In the Wells Fargo scandal, the Chief Executive Officer and the Chief Risk Officer highlighted that they were unaware of the illegal activities of the employees, which involved the creation of over 3.5 million fake bank accounts and unauthorized bill payments. The worrying issue is how the CEO and CRO were kept in the dark when all of this was happening.

Communication is with respect

One of the greatest motivators of a human being, young or old, is a feeling of being respected. Communication, whether vertical or horizontal, should carry a tone of respect. This builds self–esteem and confidence among the team, which are critical ingredients for innovation and creativity.



This kind of environment leads to:

Happier teams

Teamwork can only prosper when there is trust in teams, where employees trust each other and know that the major issue is to resolve company risks other than focusing on petty politics.

Increased employee engagement

Creating an environment where open communication is the norm, and disagreements are based on principle, encourages employees to open up, even to critical issues. The era of nursing egos is gone, and the current trend is for companies to make bold decisions in order to survive, given the ever–changing business environment, hence need for high employee engagement.

Stability of the workforce

If physiological safety is engrained in the organizational culture, employees will feel happy to work with the organization, which will minimize costs of turnover and recruitment.

Specifically, psychological safety fosters risk management in the following ways:

Reporting risk incidents

Teams gain confidence to report negative events as soon as they happen because the organization culture focuses on detection, resolution, recovering and sharing the lessons learnt rather than seeking to blame and punish the incident reporter, even before understanding the root cause of the incident.

Identification of control weaknesses

Identification of control weakness is crucial in strengthening the control systems of the organization. If the organization has an open environment, different employees can help in identifying control weaknesses and suggest stronger control measures. That means everyone body is involved in risk management, which helps to build a robust risk management culture in the organization.

Innovation & creativity

For any organization to survive in a complex environment, innovation and creativity must be at the center of their strategy. Psychological safety encourages staff to take on new challenges with the knowledge that mistakes (not repeated mistakes), in line with the company policies and procedures, are acceptable.

Dissemination of risk management information

Psychological safety reduces the barriers in sharing information between the risk teams and the rest of the organization. Ease of information dissemination is key in availing the risk department and risk owners the required facts in assessing risks, which the company is facing. Keeping control functions in the dark is a common practice in many organizations, and often risks are discovered too late, but with psychological safety this is minimized.

Risk budgeting

The debate on which risks to give high priority when allocating the risk budget is always heated, but with open and honest discussions, it is easy to identify the most critical risks.

Control self–assessment (CSA).

One of the key techniques in risk management is CSA, which involves risk owners assessing the adequacy and effectiveness of controls in their operating areas. It is expected that a self–review is subject to bias, but with psychological safety, which allows sharing of information, this process (CSA) can be enhanced by a review of the results of the CSA by control functions.

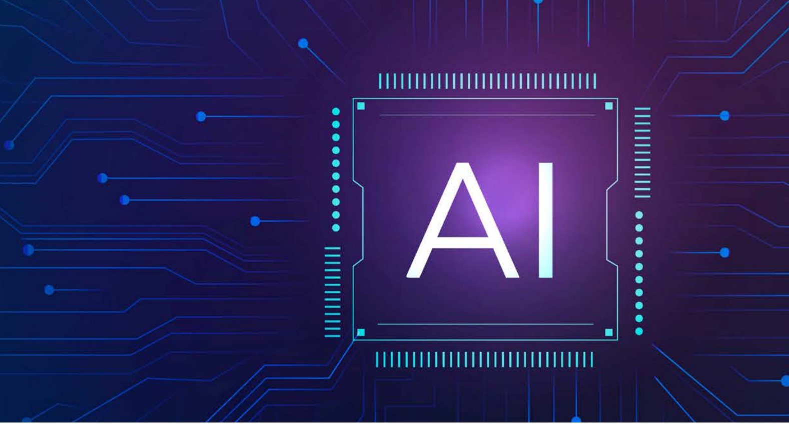
The multiple benefits of psychological safety notwithstanding, it can be abused, leading to serious problems.

In an open environment, it may be difficult to draw a line between freedom to speak out and respect for leadership. Some employees may use the open environment to undermine authority, thus compromising the mission and vision of the organization.

CONCLUSION

Given the numerous benefits of psychological safety, most importantly the fact that it creates opportunities for creativity and innovation; it is a precursor for organizational growth, especially in this dynamic and complex environment.

ENSURING IT SECURITY IN THE WORLD OF AI AND AUTOMATED SOLUTIONS



Sheba Ainembabazi
Cybersecurity Analyst,
Umeme

In today's rapidly evolving technological landscape, artificial intelligence (AI) and automated solutions are transforming various industries. From robots to self–driving cars and smart home appliances, these innovations offer unparalleled convenience and efficiency.

However, the integration of AI and automation presents security challenges that need to be addressed to safeguard against potential threats. This article explores the importance of IT security in the context of AI and automated solutions, focusing on key technologies such as the Optimus Tesla robot, Chat GPT–4, Apple's Vision Pro, and Tesla's self–driving cars.

Optimus Tesla Robot: Revolutionizing Assistance

The Optimus Tesla robot stands as a testament to the advancements in robotic technology. With its remarkable capabilities, it can navigate complex environments and performs various tasks autonomously. Its user–friendly interface allows seamless interaction and control, making it a valuable asset in diverse settings.

However, to ensure the security of such advanced robots, robust IT security measures are crucial. Safeguarding against potential hacking attempts is essential to prevent unauthorized access or malicious manipulation of the robot's functionalities.

To ensure IT security for the Optimus Tesla robot and related technologies, organizations and individuals should consider the following measures:

i) Secure communication

Implement secure communication protocols to protect data exchanged between the robot and external systems, ensuring encryption and authentication mechanisms are in place.

ii) Firmware and software updates

Regularly update the robot's firmware and software to address any security vulnerabilities and ensure it is running on the latest patches.

iii) Access controls

Implement strong access controls to restrict unauthorized physical and remote access to the robot. Use strong passwords, multi–factor authentication, and role–based access controls to limit access privileges.

iv) Intrusion detection systems

Deploy intrusion detection systems to monitor the robot's network and detect any suspicious activities or unauthorized attempts to access the system.

ChatGPT–4: Harnessing conversational AI

Chat GPT–4 represents the power of conversational AI in automated systems. It can engage in meaningful conversations, answer questions, and assist users in a wide range of tasks. However, the vast amount of personal data and sensitive information processed by these systems highlights the importance of robust data protection. Adhering to stringent security protocols, implementing encryption techniques, and regularly updating the system, are imperative to safeguard user privacy and prevent data breaches. To ensure IT security for Chat GPT–4 and similar conversational AI systems, organizations and individuals should consider the following measures:

a) Data encryption

Encrypt sensitive user data, both at rest and in transit, to protect it from unauthorized access. Use strong encryption algorithms and proper key management practices.

b) User Authentication

Implement strong user authentication mechanisms to verify the identity of users interacting with the system. This can include methods such as passwords, biometrics, or multi–factor authentication.

c) Secure data storage

Store user data in secure and encrypted databases with proper access controls to prevent unauthorized access or data leakage.

d) Regular security audits

Conduct regular security audits and penetration testing to identify and address any vulnerabilities in the system. This helps ensure that security measures are effective and up to date.

Apple's Vision Pro: Merging Digital and Physical Realms

Apple's Vision Pro is a groundbreaking product that seamlessly integrates digital content with physical space. This innovation enhances user experiences through eye, hand, and voice navigation, while also capturing spatial data. However, such technologies rely heavily on data collection and storage, emphasizing the need for stringent data security measures. Protecting personal information, securing data transfer, and implementing authentication mechanisms are essential to prevent unauthorized access and potential misuse of collected data. To ensure IT security for Apple's Vision Pro and similar technologies, organizations and individuals should consider the following measures:

i) Data minimization

Collect and store only the necessary data required for the system's functionality. Minimizing the amount of personal and other sensitive information reduces the potential impact of a data breach.

ii) Secure transmission

Implement secure communication protocols, such as HTTPS, to encrypt data during transmission between the device and external systems. This prevents unauthorized interception and data tampering.

iii) Privacy by design

Incorporate privacy and security considerations into the design and development of the product and follow privacy frameworks and principles to ensure user privacy.

iv) Regular security assessments

Conduct regular security assessments and vulnerability scans to identify and address any weaknesses in the system. This helps maintain the integrity and security of the collected data.

Tesla's Self–Driving cars revolutionizing transportation.

Tesla's Autopilot feature has paved a way for self–driving cars, offering enhanced safety, reduced congestion, and minimizes carbon emission. However, the reliance on interconnected systems and extensive data processing, raises concerns about potential cybersecurity risks.

Protecting autonomous vehicles from malicious attacks is crucial to ensure the safety of passengers and prevent unauthorized control or manipulation of critical systems.

To ensure IT security for self–driving cars like Tesla's Autopilot, organizations and individuals should consider the following measures:

a) Secure vehicle architecture

Implement a secure vehicle architecture that isolates critical systems from external communication channels. Employ network segmentation and firewall mechanisms to prevent unauthorized access to critical vehicle functions.

b) Secure over–the–air updates

Ensure that over–the–air (OTA) software updates for autonomous vehicles are delivered securely and implement robust encryption and authentication mechanisms to prevent unauthorized or malicious updates.

c) Intrusion detection systems

Deploy intrusion detection systems within the vehicle's network to monitor and identify any suspicious activities or attempts to compromise the system's security.

d) Threat modeling and risk assessment

Conduct comprehensive threat modeling and risk assessments to identify potential vulnerabilities and implement appropriate security controls to mitigate them.

Conclusion

Overall, the integration of AI and automation into various industries brings both convenience and security challenges. Technologies like the Optimus Tesla robot, Chat GPT–4, Apple's Vision Pro, and Tesla's self–driving cars showcase the potential of AI but also require robust IT security measures. By prioritizing IT security, we can leverage the benefits of AI and automation while ensuring a safer and more secure technological landscape.

MANAGING THIRD PARTY RISK EFFECTIVELY

Stephen Babigumira
Information Security Manager,
National Social Security Fund

Covid–19 affected nearly every organization in the world in different ways and at varying degrees of impact. In extreme cases, those that were unable to innovate and adapt to the changing environment were forced to close business. Those that survived, some had to make significant structural changes, including downsizing, and outsourcing some of their operational functions to third parties.

A third party is an individual or entity from whom an organization gets a service or a product to deliver its products or services. Third–party risk is the likelihood that the third party may fail to keep their promise, resulting in the affected individual or entity failing to deliver its products or service.

The rationale behind hiring third parties is to leverage the external expertise and other capabilities that may not be existent internally in the organization. That shortens the process that would be required to develop such expertise/capabilities and lessens the associated high short–term costs of doing so.

However, third parties come with several risks, and to effectively manage risk throughout third–party ecosystem can be difficult, particularly for large organizations. Nonetheless, there are various steps you can take to better understand your risk environment and mitigate the impact of potential third–party risk.

Below are some of the risks associated with third parties and how to mitigate them.

i) Disclosure of confidential information

Third parties such as IT vendors, contractors, etc, may be given access to the organization's internal systems to enable them to accomplish their contractual duties. In the process, they may gain access to the organization's confidential information, and if they are not ethical, they may disclose such information for personal gain or out of sheer negligence.

To mitigate this, organizations need to sign a non–disclosure agreement with the vendors before granting them such access. Secondly, access should be granted on the principle of least privilege, whereby the vendor's access is limited to only applications or modules he/she requires to execute his/her duties. Thirdly, the vendors' actions in the systems should be monitored regularly.

ii) Integration risk

To improve operational efficiency and quicken service delivery, many organizations integrate their systems with third party systems. The risk is that, this introduces new vulnerabilities (weak link) into the organization's security ecosystem, if the third party's security infrastructure is weak. These weaknesses in the third party's systems may be exploited by a malicious actor to gain access to your organization's sensitive information.

Third–party data breaches are becoming increasingly common as technology continues to make it easier for businesses to connect. The increase in these kinds of attacks is not likely to slow down in the near future, because malicious actors are increasingly pursuing a strategy of leveraging one successful attack to damage more companies in the supply chain, this has been evident mostly in software companies.

Some of the notable data breaches that have involved third parties in the recent past include:

a) Okta Third–Party Data Breach

In March 2022, Okta, a U.S.–based identity and access management platform, reported that one of the third–party vendors they were dealing with experienced an attack that resulted in a data breach, impacting approximately 2.5% of their customer base.

b) Mercedes–Benz

In June 2021, Mercedes–Benz reported that approximately 1.6 million records of customer sensitive information were leaked through a third–party vendor's cloud storage platform.

c) Eye Care Leaders Ransomware Attack

In December 2021, a ransomware attack on Eye Care Leaders' EMR (electronic medical records) exposed data of 3.7 million people to threat actors. Several health–care providers had to notify millions of patients that their medical records had been compromised following an attack on a third–party electronic medical record (EMR) platform.

To address such third–party risks arising from integration of systems, the organization needs to:

Consider information security during sourcing and selection of suppliers. As your IT systems become increasingly integrated with third parties, it is critical to consider information security during vendor sourcing and selection. Organizations should give precedence to those with demonstrable mature information security risk management practices.

Consider leveraging third–party risk management softwares during sourcing and selection processes, which come with preloaded cybersecurity risk data.

In addition, you should practice proactive, external third–party monitoring for all vendors that deal with your confidential information. Organizations change their information security programs over time, and what was originally reported on their vendor risk assessment questionnaire may not hold true a few months later.

Lastly, you should pay attention to the third–party offboarding process. This is one of the most essential elements of preventing third–party data breaches. Ensure that as part of winding up the relationship with the third party, all access and permissions are revoked and data retention requirements are honored.

iii) Reputation risk

If the products and/or services from the third party, which are inputs into the organization's product development or service delivery, are substandard, the quality of the organization's products or services will be compromised, affecting the image of the organization.

To mitigate this, the organization should determine service and product standards, which should be incorporated in the agreement with the third party.

iv) Fraud risk

Gaining access to the organization's systems gives the third party an opportunity to explore the weaknesses within the organization's system, which he/she can exploit to commit fraud.
One of the control measures for this risk is to ensure that access to the systems is granted based on the principle of least privilege.

Secondly, the vendors' actions in the systems should be monitored regularly.

Thirdly and most importantly, the organization needs to conduct due diligence before onboarding the third party. This helps to assess the integrity of the potential vendor or supplier before dealing with them.

v) Compliance risk

If the contractual relationship between the organization and the third party is such that the third party is required to process personal data on behalf of the organization, this may expose the organization to litigation, arising out of data breach in the context of the applicable Data protection and privacy laws, such as the Data protection and privacy Act 2019 of Uganda. This will arise if the third party does not have adequate and effective framework to ensure full compliance with the Act.

To mitigate this risk, the third party should be sensitized on the need to comply with the Act. The organization should ensure that the third party develops and implements appropriate compliance frameworks. You could require vendors to independently verify their compliance to the applicable laws and regulations.

vi) Business continuity risk

Over reliance on a single third party can create serious business continuity risk. If for instance, 70% of your organization's operations are supported by a single supplier, when that supplier experiences a major problem, the organization will be significantly impacted, and may not be able to continue its operations.

For example, in February 2022, Toyota announced that they were suspending operations at 14 manufacturing plants in Japan for a day due to a system failure at Kojima Industries, one of its suppliers. It was also reported that other partners of Toyota, including Hino Motors and Daihatsu Motor, were also affected by the shutdown.

The mitigation measure for this risk is to diversify the sources of supply– have multiple suppliers. Secondly, for the big suppliers, have a formal business continuity plan with them.

vii) Operational risk

Oftentimes, time management is a big challenge when dealing with third parties. Since the organization is not able to supervise the staff of the third party directly, the third party may not comply with the time requirement of the organization (their client). The delays will affect the operations of the organization.

The control for this risk is a stipulation, in the contract, of the timelines and penalties for non–compliance with the delivery timelines.

CONCLUSION

Dealing with third parties is inevitable because no organization can exist in a vacuum– it cannot have all the resources and expertise that it needs internally. Third parties play a significant role in bridging that gap. That notwithstanding, organizations need to first of all be aware that there are various risks associated with dealing with third parties, and secondly, assess and treat the risks appropriately, so as to have a beneficial third–party relationship.

PRIORITIZING ESG FOR SUSTAINABLE GROWTH

Ian Mugisha
Board Chair,
Certified Risk Management Professionals (CRMP)

For those who have appreciated ESG principles, it is no longer debatable whether ESG factors significantly impact businesses. The challenge is that several businesses still view the implementation of ESG frameworks as far detached from their primary role of increasing "shareholder value". This is ironic because the implementation of ESG frameworks ensures sustainable value addition.

ESG refers to environmental, social, and governance factors, which can have a significant impact on a company's performance. Before I tackle the importance of ESG in ensuring business growth and sustainability, we need to be on the same page regarding the ESG factors, starting with environmental factors.

Environmental Factors: The effects of an organization's operations on the environment are referred to as environmental factors.

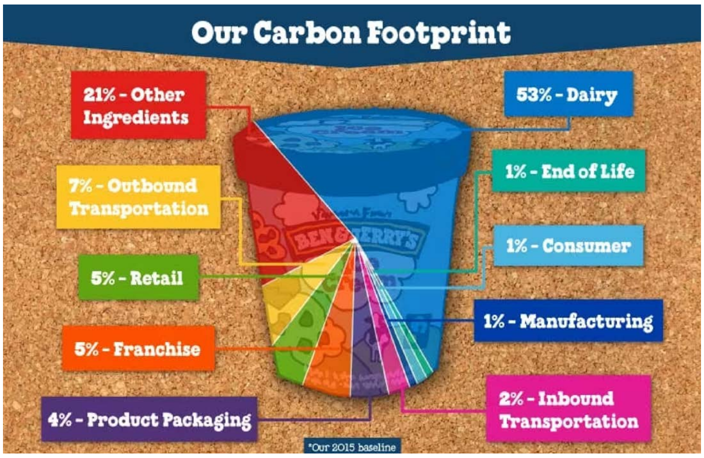
The negative effects of an organization's operations that cause environmental degradation such as deforestation, pollution, contamination of water bodies, etc., can generate a serious backlash from the population, in form of a boycott of its products, and in extreme cases, vandalism or destruction of the organization's properties. On the other hand, positive effects of the organization's operations enhance its value, through improved brand equity, which translates into increased revenue and balance sheet growth.

The Ndere Cultural Centre is one instance of a company in Uganda that values environmental sustainability. The institution prioritizes ecological practices, while promoting cultural heritage and providing traditional dance performances. They gather rainwater to use in their gardens, generate power using solar panels, and manage waste using a composting system. In addition to promoting the preservation of Uganda's natural resources, the Ndere Cultural Centre's emphasis on sustainability has assisted in drawing tourists and visitors, who respect ecologically friendly practices.

Social Factors: The social impact of an organization's operations is referred to as a social factor. Just like environmental factors, positive social factors enhance the organization's value, while negative social factors erode the organisation's value.

Ben & Jerry's (BJ) is a fantastic illustration of a business with a strong commitment to doing good in the world. They are activists for a better world with a social mission that "seeks to eliminate injustices in our communities by integrating these concerns into our day–to–day business activities".

Below is a chart with an illustration of BJ's Carbon footprint.



Source: Ben & Jerry's website: An illustration of a Ben & Jerry's ice cream pint is used as a pie chart to show Ben & Jerry's carbon footprint.

BJ believes doing something starts with knowing the baseline, and currently their manufacturing and retail operations contribute less than 6% to their baseline footprint, mostly because they have tackled it head–on. They are nearly at their 2025 goal of 100% renewable electricity for their global manufacturing operations.

Divine Chocolate, a chocolate producer in Ghana, is a company that prioritizes social impact in all aspects of business. The company's goal is to uplift the livelihoods of small–scale cocoa growers. To ensure that farmers receive fair prices for their cocoa beans and a voice in the business's decision–making, Divine Chocolate collaborates with cocoa farmers. Additionally, Divine Chocolate makes investments in social initiatives, including healthcare, education, and training, which help communities in West Africa that harvest cocoa.

Divine Chocolate has developed a devoted following of customers for their ethical standards; this has seen the brand develop various partnerships with huge brands that have led to significant growth of the company, expanding its operations overseas, such as in the United States of America.

As mentioned above, if the organization's operations cause negative social impact, the reaction from the population may be detrimental to the organization. In the 1990s, Nike faced a boycott because of complaints about its treatment of workers in foreign factories. Nike was compelled to move to improve the working conditions in its factories because of the boycotts and demonstrations, which emphasized the significance of fair labour practices in Nike's global supply chains. This is a classic example of how ESG issues can have serious ramifications on a business.

Nike was forced to review its policy regarding ESG matters. Nike has since become known as a pioneer in ethical and sustainable business practices, and its initiatives to improve working conditions throughout its supply chain have inspired other businesses in the sector.

In the recent past (2020), civil rights organisations boycotted Facebook in protest of the company's management of hate speech and disinformation on its platform. Thousands of businesses joined the campaign and ceased advertising on Facebook for at least a month. As the boycott rapidly gained momentum, revenue and stock price of Facebook were significantly impacted. In response, Facebook introduced new guidelines to address hate speech and disinformation and established a task group for civil rights to oversee its initiatives.

In Uganda, similar incidents involving boycotts or protests against companies over ESG issues have occurred. The debate over building a hydroelectric dam on the Nile River in Murchison Falls National Park is one such incidents. Environmental organizations and citizens have criticized the project, voicing concerns about its effects on the biodiversity of the park and the displacement of adjacent populations.

These incidents highlight the significance of ESG (environmental, social, and governance) factors for any organisation.

Governance Factors: These are factors that relate to the internal management systems of an organization. Effective risk management, accountability, and transparency are all attributes of good governance practices. To ensure good governance practices, several private sector organizations in Uganda have established governance structures such as boards of directors, audit committees, and risk management roles.

However, issues of corruption, embezzlement of funds, nepotism, and other vices, are perceived to be prevalent, especially in government institutions. The Ugandan government has put in place a number of structures to encourage effective governance. For instance, the Inspectorate of Government is in charge of looking into instances of corruption and upholding morality and integrity in government agencies. The Human Rights Commission promotes and defends human rights in Uganda, while the Auditor General is charged with ensuring accountability and openness in the use of public funds.

The growth and sustainability of an enterprise largely depends on its governance systems. An institution's leadership is accountable for its success or failure. In Uganda, most private enterprises do not live beyond their first generation of leadership. On the contrary, in Asia the majority of family–owned businesses outlive their founders.

So, what can businesses do for sustainability? Satya Nadella, the CEO of Microsoft, stated, "We strive for a culture of transparency, accountability, and integrity in everything we do."

Microsoft has been successful in establishing a solid reputation for sound governance practices, which has aided the business in luring investors and clients who value accountability and openness.

Organisations should prioritize ESG considerations for a number of reasons:

Firstly, businesses that put an emphasis on ESG considerations typically have a good reputation, which can draw in clients, investors, and employees.

Secondly, businesses prioritizing ESG factors are more likely to minimize critical risks, such as societal unrest, environmental catastrophes, and governance failures.

Thirdly, ESG factors can aid organisations in developing stakeholder trust and confidence, which is crucial for long–term success.

Fourthly, ESG aspects are crucial to an organization's long–term success. For organisations to succeed in the modern world, environmental sustainability, social responsibility, and good governance practices are no longer optional.

Companies that give priority to ESG considerations are more likely to prosper, as people become more aware of how their actions affect the environment, society, and governance. Mahatma Gandhi once said, "The future depends on what we do in the present." Companies that give ESG concerns a high priority today are setting the groundwork for a better future, for both, the rest of the world and themselves.

Now is the time to act on environmental sustainability, social responsibility, and good governance (ESG), by either pushing for them in your workplace or investing in firms that do so. We can all contribute to creating a better future for the earth and ourselves, by supporting ESG. Never forget that our actions today will determine our future.

CASUAL
LABOURERS
SUB CONTRACT
WORKERS
SMALL
EMPLOYERS
BARUNGI TEA ESTATE
NSSF
a better life

AGILITY IN RISK MANAGEMENT.

Baguma Adolf Kaija
Operational Risk Manager,
National Social Security Fund

The current business environment is more complex than ever before; the changing dynamics, which include but not limited to demographics, customer expectations, competition, emerging technologies, statutory requirements, geopolitical issues, etc., have increased growth and profitability uncertainties in business.

It is a period where even businesses with very healthy financial footing can collapse due to the complex and highly intertwined business environments. It is a situation where, only the 'smartest' and those who practice the most agile risk management techniques and can quickly adapt to the changes in the environment will survive.

These changes are key drivers of heightened risk exposure for organizations, which in turn create new risks or lead to mutation of existing risks, that could potentially lead to businesses not achieving their objectives.
Because of the precariously changing environment, organizations need to be alert and redefine their risk management approaches to keep pace with the changes in the business dynamics and adapt to the complexities, in order to remain relevant in the marketplace. This requires agility and resilience.

Agility in the context of risk management, is the organization's ability to quickly change and adapt risk management frameworks and practices to respond to the ever–changing business dynamics.

Risk agility requires businesses to be proactive in their approach to risk management and prevent risks from materializing, to minimize the disruptions to the flow of business operations rather than crossing fingers in the hope that the risks will eventually go away. Businesses that wait until risks have reached intolerable levels, exhibit a reactive approach to risk management, which perpetuates a vicious cycle of risk materialization.

Meanwhile, businesses that adopt a more agile approach by setting predictive key risk indicators (KRIs) that provide them with early warning signals, can act fast and make the appropriate changes to minimize the impact of any risks that may materialize.

Let's now delve into some of the specific approaches or interventions that organizations could adopt to have a more agile and robust risk management framework.

Profile all the business risks

For better risk oversight, businesses must build a comprehensive risk universe, commonly called a risk register, as a first step into an agile risk culture. This will act as a library of all the key risks and associated opportunities that could have an impact on the business, and should include a broad–spectrum of strategic risk, reputational risk, financial, operational, and other categories that an organization may deem fit.

These risks should be identified from business processes, transactions and operational data but not just profiling generic risks. Key Risk Indicators (KRIs) and risk tolerance limits should be set to help management know when risks are about to materialize, thereby enabling action to be taken early, and that is, what an agile approach to risk management is all about. Setting KRIs and tolerance limits is in line with Adam Smith's assertion that; An agile approach to risk management enables an organization to;

- Set controls to flag areas of concern, including missed deadlines, anomalies in data, budget overspending, too many incidents, or when KRIs reach intolerable levels.

- Monitor risk over a period and understand the behavior of each risk.
- Get a holistic view of the organization's overall risk profile using dashboards and regular reports.

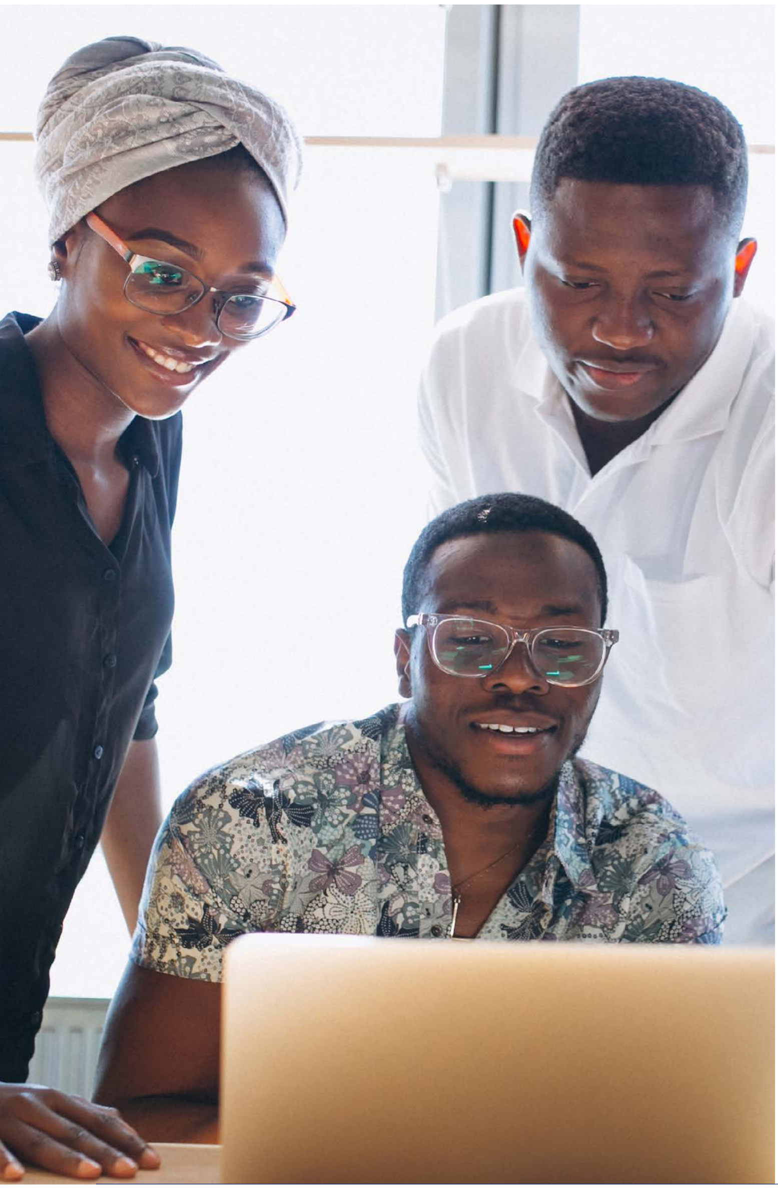
Act with agility to respond to risks

Armed with information collected during the risk profiling exercise, businesses will be well equipped to anticipate risk and understand the potential likelihood and impact, enabling them to build contingency plans. Equipped with this information, an organization should be able to act with agility in responding to risk.

Therefore, for ultimate agility, businesses should consider integrating risk management processes with strategy planning, policy management and incident reporting processes.

Build a robust business continuity and disaster recovery framework.

Another way organizations can be risk–agile, is by building effective business continuity and disaster recovery response capabilities to respond to unforeseen events. Business continuity planning (BCP) is a proactive business process that helps a company understand potential threats, vulnerabilities, and weaknesses to its operations in times of a crisis. On the other hand, Disaster recovery (DR) is an organization's ability to respond to and recover from an event that negatively affects business operations, and be able to regain use of critical systems and processes following a disaster.



The creation of a business continuity and disaster recovery program ensures that a company's management can react quickly and efficiently to business interruptions.

BCP is a very important concept in risk management because it provides an organization with the capability to continue the delivery of products or services at pre–defined acceptable levels following a disruptive event.

It is through Business continuity planning, that an organization can create systems and infrastructure for continuity and recovery in case a disruptive incident happens.

In establishing a business continuity framework, it is important that the organization conducts a business impact assessment (BIA). The BIA will identify critical and non–critical activities across the enterprise, such that the critical business activities are prioritized in the recovery process.

To assess the effectiveness of the BC/DR plan, the organization must exercise the plan regularly. The RTOs (Recovery Time Objectives), which are the maximum time it takes to restore a technology system following a disaster, act as key performance indicators (KPIs). Compliance with the agreed RTOs is an indicator that the BC/DR framework is working effectively. In case the organization fails to achieve the target RTOs, the causes of failure should be analyzed and addressed.

Embedding Risk Culture

An agile and effective risk management requires management to ensure that a positive risk culture takes root throughout the organization. This can be done if management or those charged with governance set the right tone at the top, by showing visible willingness to let values drive decisions above other factors.

The tone at the top determines an organization's ethical climate upon which the culture of an enterprise is built. A positive risk culture increases compliance with policies and procedures and raises the level of risk consciousness across the organization. A well–defined risk culture requires individuals within the organization and its external stakeholders to be predisposed towards risk consciousness, by taking deliberate initiatives, including sensitization about the importance of effective risk management, the need for reporting risk events to those in charge, and transparent risk information flow across all departments, among other initiatives.

CONCLUSION

As the business environment becomes more complex and dynamic, the risk landscape becomes more rugged. Success will not only depend on the organization's agility to develop appropriate business strategy, but on its agility in identifying, assessing, and responding to risks that affect the business strategy. Chief Risk Officers (CROs) should validate the assumptions underlying any business strategy or initiative and use this to advise the business on the appropriate risk management framework. An agile risk management approach provides valuable information for anticipating what might go wrong, analyzing, and evaluating potential effects, and identifying the best response actions.

EMPLOYER OBLIGATIONS IN DISASTER RESPONSE

Sowati Sowali Mukose
Head of Risk,
Tropical Bank Limited

Emergencies, disasters and hazards can occur at any time without warning. The more prepared an organization is, the better it is in responding to an emergency, which minimizes panic and confusion, when a disaster occurs.
The requirements for emergency preparedness and response are described in the occupational safety and health Act, 2006 (Laws of Uganda), which requires employers to have plans for responding to general emergencies in the workplace.

Assessing the impact of a potential natural disaster and putting in place a mechanism to minimize the impact it may have on a business, can help keep employees safe and reduce business disruptions. The Act expressly requires employers to have written emergency response plans that include preparedness and response measures. There are different kinds of emergency plans, procedures and safety information. Some give instructions on how to use a control measure to prevent any injuries or fatalities, like a lifejacket, warning signs, emergency exits or SOS lights. Others provide information on what to do, what not to do or how to leave a building in case of a dangerous or catastrophic event, such as a fire outbreak or a hazardous situation. These include maps or evacuation plans and brochures, alarm instructions, what to do when emergency alerts happen, etc. It is recommended that all organizations develop effective emergency response plans for their workplace, no matter which jurisdiction they are in.

The emergency response plan

This plan should include:
- Policies, practices and procedures
- Communication
- Training and sesnsitization
- Monitoring and supervision
- Review and updating

The plan should identify potential hazards and provide emergency guidelines, which should be periodically reviewed. It is important that all employees, customers and the public at large know about these plans and understand them. At a minimum, an emergency action plan must include the following:

- A preferred method for reporting fires and other emergencies
- An evacuation policy and procedure
- Emergency escape procedures and route assignments, such as floor plans, workplace maps and safe or refugee areas
- Names, titles, departments and telephone numbers of individuals both within and outside your company, to contact for additional information or explanation of duties and responsibilities under the emergency plan.
- Procedures for employees who remain to perform or shut down critical operations, operate fire extinguishers or perform other essential services that cannot be shut down for every emergency alarm before evacuating.
- Rescue and medical or first aid duties for any workers designated to perform them.
- The site of an alternative communications centre to be used in the event of a fire or explosion.
- A secure location, on or offsite, to store originals or duplicate copies of accounting records, legal documents, your employees' emergency contact lists and other essential records.
- A way to alert customers and employees, including differently–abled customers and employees to evacuate or take other action.

In addition, organizations should:
- Establish procedures for assisting differently–abled people and people who do not speak English.
- Provide a plan or safety information in an accessible format that meets the needs of persons who are differently–abled, so that they can be aware of the organization's emergency procedures.
- Post evacuation procedures, where employees can read them.
- Consider designating an assembly location and procedures to account for all persons and employees after an evacuation.
- All workers should be instructed and trained on the company's emergency response policies, practices and procedures, as well as potential threats and hazards.
- Workers designated to perform specific duties under, for example, a fire response plan such as evacuation or putting out the fire, etc., must receive special training. Workers assigned to firefighting duties should

have adequate training by a qualified instructor in fire suppression methods, fire prevention, emergency procedures, organization and chain of command, firefighting crew safety and communications.

Management of organizations should also think of holding emergency drills, at least once a year, to ensure that employees know what to do in case of an emergency, and to test the effectiveness of emergency exit routes and procedures.

Organizations should conduct training sessions at least once a year or whenever they:

- Hire new employees.
- Designate evacuation wardens or others with special assignments.
- Introduce new equipment, materials, or processes.
- Find, through exercises, that employee performance during an emergency drill needs to be improved.

Communicating with employees about a disastrous event

Communication before, during and after a disastrous event or other emergency, is critical, and plans for such communication should be included in the emergency action plan. Employees should know and understand how to communicate with their employer and how to obtain necessary information in the event of an emergency. It is difficult to think clearly in the midst of chaos, so it is important for employees to know in advance what they are expected to do.

Employers should maintain current contact information for all employees and have a process in place to ensure it is routinely updated. Some organizations implement a communication/call tree, where a few employees are designated to each call a list of people, each of whom calls another list of people, and so on until everyone has been contacted. Other employers use technology to send out a recorded message or group text, while some establish a call–in number for employees to save and use during emergencies. Whatever procedure the employer chooses, someone should be specifically charged with ensuring that it is followed during an emergency and that all employees are contacted.

The bottom line for employers is to plan ahead and not wait until a disaster strikes. A well–written emergency response plan can protect employees and the employer, and help to minimize confusion during and after an emergency. It is better to be safe than sorry!

HURDLES PENSION FUNDS ENCOUNTER IN EXECUTING THEIR MANDATE

Masiga Robert
Investment Risk Specialist,
National Social Security Fund

For most employed people, their source of income is salary, and when they retire, they become very vulnerable to extreme poverty. Pension funds are established to provide a safety net for retirees, as an income replacement mechanism. A pension fund is an accumulation of funds that are to be paid out to employees on retirement.

Although pension funds play a significant role in income replacement for retirees and the overall economic growth, they face numerous challenges, as explained later in this article.

Typically, there are two major categories of pension funds, that is, Defined Contributions and Defined Benefits Pension schemes, which can either be public or private:

Public pension fund: This is one that is regulated under public sector law. It is a social security plan administered by central, state, local government, or municipal authorities as well as other public–sector bodies, depending on the different jurisdictions.

Private pension fund: This is regulated under private sector law, where individuals contribute a percentage or a fixed sum from their earnings to the fund, and when they retire, they are paid a lumpsum of their contributions plus accrued investment returns or an annuity.

The Need for Pension Schemes

Pension schemes are major fallbacks for many retirees, whether in public or private sector. This is generally so, because during the employment life, majority of the workers focus on the short to medium term needs and little, if any consideration, is placed on long term needs after retirement.

In many countries, pension funds are vibrant and significantly contribute to the countries' socio–economic development, as they guarantee retirees' better standard of living after their active service. However, pension funds face several challenges or risks as explained below.

Challenges faced by Pension Funds

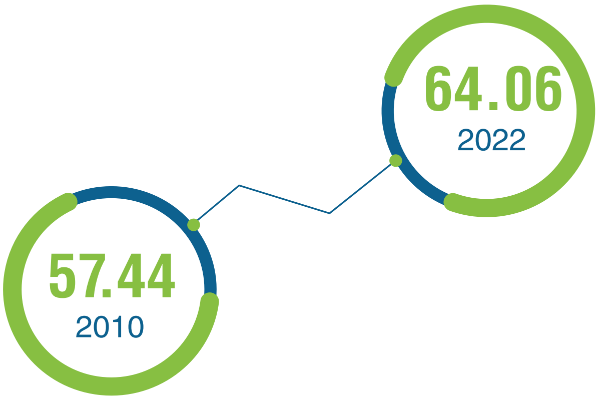
To begin with, pension funds are set–up for particular purposes, the main goal of which is to ensure there will be enough money to cover the pensions of employees after their retirement in the future.

Longevity risk

Pension funds, especially defined benefits schemes (DBs), enroll members and commit to pay them benefits from the time of retirement until death. The higher the life expectancy, the greater the pension liability, thus creating a longevity risk to the pension fund.

Despite the rampant epidemics and pandemics, the general health and wellbeing of the population (plan participants) have on average improved globally. For instance, according to macrotrends.net, at a global level, life expectancy was estimated at 72.98 years in 2022 compared to 69.7 years in 2010. The trend is not different for Uganda, whose life expectancy was 64.06 years in 2022 compared to 57.44 years in 2010.

Life Expectancy in Uganda



This means that people are living longer than ever before, growing the size of the liabilities that pension funds have to meet, thus increasing longevity risk for pension funds.

Estimating defined benefit liabilities

The biggest challenge associated with offering a DB pension plan, is estimating its pension liability, referred to as projected benefit obligation (PBO). This estimation is based on a retirement benefit formular, with numerous assumptions such as employee salary growth rate, estimated length of working period, length of time employee will receive a monthly retirement benefit, the number of years employee is expected to work, among others.

These assumptions change from time to time in accordance with actuarial principles. As a result, the PBO changes from time to time, making its estimation extremely difficult. For instance, it is difficult to estimate with certainty, how long an employee will work for a company, especially with the increasing phenomenon of quiet quitting.

Given this background, the liability increasingly becomes difficult to estimate. This presents a challenge to pension funds in determining pension benefit obligations.

Accounting issues

The accounting treatment of a pension fund's assets and liabilities varies across jurisdictions. According to an article, 'Defined–Benefit Plan: Rise, Fall, and Complexities', by Troy Adkins, in some countries such as the US, under financial accounting standards board (FASB) 87, off–balance sheet accounting of pension assets and liabilities is permitted.

PBO and plan contributions are not included on the balance sheet, and instead, it's the netted figure between assets and liabilities that is included. The net figure is an asset if the plan is overfunded and a liability if the plan is underfunded.

This flexibility in accounting treatment, renders financial ratio analysis difficult for stakeholders and can lead to wrong conclusions about a pension scheme's financial condition.

Mismatch between assets and liabilities.

A mismatch between asset and liability horizons can be a serious problem for pension funds. Usually, pension fund liabilities are long term in nature (defined by law); a proper asset allocation would require that a pension fund invests in long term assets. However, if for instance, money is invested in short term assets, which usually have low returns, the pension fund may not have adequate funds to settle long term liabilities when they are due.

Changes in legal/regulatory environment

Pension funds are established by law, which defines their mandates. However, due to political, economic, and social dynamics, societal needs evolve, which may necessitate amendment of existing legislations to carter for stakeholder demands. The amendment(s), if successful, can completely change the operating environment of the pension funds.

The changes may require considerable resources in terms of manpower, time, and finances. As a result, some activities may have to wait a little longer until the requirements of the law are met.

A clear example here could be the recent amendment of the NSSF Act. Policies had to be revised to align them with the new requirements of the law. Furthermore, the amendment resulted into emergence of a benefit type (Midterm access) that allowed members access their savings, which was a good intervention for the members in the short–term, following the economic disruption caused by Covid-19.

However, this affected the liquidity of the Fund. About UGX 618 billion were paid within three months (March – May 2022), of which 425 billion were for midterm access. Compared to UGX 103bn that was paid the previous year in the same period, this was an increase of UGX 515bn (500%).

The experience of NSSF Uganda is worth celebrating, for the resilience to handle the emergence of midterm benefits. Other global financial institutions' stories are quite appalling. Take the example of Silicon Valley Bank (SVB) in the USA, that had to wind up business as a result of a policy change regarding interest rates.

According to the article, "What happened to Silcon Valley Bank", by Erin Gobler on Investopedia, the Fed had for long kept the policy rate low since the financial crisis of 2007/2008. When the rate was revised upward, SVB invested in long term treasuries to earn the high rate.

They kept a small proportion in short term positions which failed to match the short term needs of their clients. SVB collapsed after it failed to raise $2 billion in capital to shore up its financial position, due to mismatched positions of deposits for clients and assets that had been invested in long term treasuries. SVB faced a bank run, as clients withdrew their deposits amid rumors of its insolvency.

Limited investment opportunities

Pension funds around the globe have the latitude to invest in any market once the risk–return continuum is satisfied. This mostly manifests in developed and emerging markets.

The story is quite different when it comes to frontier or under–developed markets, where regulations and policies are stringent, not to allow investments in certain markets outside particular regions.

For the NSSF Uganda, investment is limited to East African region, which cannot absorb the available investible funds, thus limiting the returns to members.

Missing, incorrect or inconsistent data.

One of the critical success factors of pension management, is accurate and relevant data, especially member data. Data integrity issue is a common problem in pension funds, especially in developing countries. Pension funds keep member data for a long period of time, which poses a challenge of ensuring consistence and accuracy of data.

For instance, if there are no regular updates regarding births and deaths, it would be difficult to know the right dependents of a particular member in case of death.

In summary, there is no doubt that pension funds play a pivotal role in socio–economic development globally, but their operating environment is characterized by various challenges, which are both internal and external. Effort is needed by pension managers and relevant authorities, like regulators, to enable the pension funds overcome the challenges and create value for the members and the economy at large.

NAVIGATING THE RISK OF SELECTING A FINANCIAL ADVISOR.

Aisha Nakanwagi
Customer Financial Advisor,
National Social Security Fund

The danger of following a wrong financial advice could be an obstacle to an individual's wealth building journey, and in most cases emanates from the poor selection of a financial mentor. More often than not, individuals seek financial advice from motivational speakers rather than financial advisors, which often results into receiving half–baked or wrong financial advice.

Motivational speakers typically focus on inspiring and motivating individuals to act towards achieving their goals, including financial goals. They often share personal success stories and provide general advice on how to change one's mindset, habits, and overall attitude towards money.

However, they may not necessarily have the required expertise and knowledge in specific financial matters, such as investing, budgeting, or retirement planning.

On the other hand, financial advisors typically have formal education and training in finance, economics, accounting, or related fields, and provide personalized advice and recommendations based on their client's financial situations, goals, risk tolerance and constraints. Constraints mainly include;

Time horizon – Highlights the different life stages remaining in a person's life. Advice is different at different stages.

Tax – Tax advice depends mainly on the source of income, as noncompliance with tax laws can erode one's investments.

Liquidity needs– Living expenses, school fees, medical expenses, etc., can affect your investment portfolio if not well planned.

Unique circumstance– Every individual is different, and so is their life story. There is need to incorporate your unique circumstances into your investment plan.

Financial advisors may also help clients develop financial plans, manage their investments, and navigate complex financial products and regulations. While there may be some overlap between the services provided by motivational speakers and financial advisors, they typically target different audiences and serve different needs.

For instance, someone who is struggling with debt or wants to invest for the first time, may benefit more from working with a financial advisor, who can provide tailored guidance and recommendations based on clients' specific situation. While someone who needs motivation and inspiration to take control of their finances may find a motivational speaker's message more helpful.

Wrong financial advice can have significant negative effects on individuals and their financial well–being. Below are some potential consequences;

Financial losses

Following incorrect advice can lead to financial losses. For example, investing in risky assets based on inappropriate recommendations can result in the loss of the principal invested or reduced returns. Making poor decisions regarding budgeting, debt management, or tax planning can also lead to financial setbacks.

Missed opportunities

Wrong financial advice may cause individuals to miss opportunities for growth and wealth accumulation. This could involve avoiding profitable investments or failing to take advantage of tax–saving strategies, retirement planning options, or other financial tools that could have helped secure a better financial future.

Increased debt and financial stress

Poor financial advice may lead individuals to accumulate unnecessary debt or fail to manage existing debt effectively. This can result in increased financial stress, as individuals struggle to meet their financial obligations, leading to penalties, higher interest rates, among others.

Impacted retirement plans

Inaccurate advice regarding retirement planning can significantly affect individuals' ability to save and prepare for their post–employment years. Inadequate contributions to retirement accounts or poor investment decisions can leave individuals with insufficient funds for retirement.

Emotional and psychological impact

Financial challenges resulting from wrong advice can lead to emotional distress, anxiety, and depression. The stress of dealing with financial difficulties, that is, loss of money, unfulfilled financial goals, etc., can strain relationships, impact mental well–being, and hinder overall quality of life.

Trust and confidence erosion

Receiving incorrect financial advice can erode trust in financial advisors. It can make individuals skeptical or reluctant to seek further advice, hindering their ability to make informed decisions and seek appropriate assistance.
To prevent the above problems, one has to be careful when selecting a financial advisor and has to assess him/her against the following key qualities.

Expertise and knowledge

A good financial advisor should have a deep understanding of various financial concepts, investment strategies, tax regulations, and financial products. They should continually update their knowledge and stay informed about the latest trends and changes in the financial industry.

Good communication skills

A financial advisor should be an effective communicator, capable of explaining complex financial concepts in a clear and understandable manner. They should listen attentively to their clients, understand their goals and concerns, and communicate recommendations or strategies in a way that aligns with their clients' preferences and level of financial knowledge.

Trustworthiness and reliability

Trust is essential in the advisor–client relationship. A good financial advisor should be trustworthy, reliable, and transparent in their actions and recommendations. They should honor their commitments, provide accurate information, and keep client information confidential.

Professionalism and ethics

It is crucial for a financial advisor to uphold high ethical standards and act in the best interest of their clients. They should prioritize the client's financial well–being and disclose any potential conflicts of interest. A good financial advisor adheres to a professional code of ethics and puts their client's needs first.

Experience and track record

Experience is an invaluable asset in financial consultancy. Look for an advisor with a proven track record of successfully helping clients achieve their financial goals. Experienced advisors have likely encountered a wide range of financial scenarios and can draw from their past experiences to guide you effectively.

Analytical and problem–solving skills

Financial planning often involves analyzing complex data, evaluating investment options, and finding solutions to financial challenges. A good financial advisor should possess strong analytical skills to assess various factors, identify risks, and make informed decisions that align with their clients' goals.

Continuous learning

The financial industry is ever evolving, with new regulations, investment products, and market trends emerging regularly. A good financial advisor demonstrates a commitment to continuous learning, staying updated with industry changes, and expanding their knowledge to provide the best possible advice to their clients.

Client–centric approach

Each client has unique financial goals, risk tolerance, and circumstances. A good financial advisor tailors their advice and recommendations to the specific needs of each client. They take the time to understand their clients' goals, aspirations, and concerns, and develop personalized strategies to help them achieve their objectives.

In conclusion, inappropriate financial advice can result in financial loss and in a worst–case scenario, bankruptcy, due to poor allocation of resources. An individual must be careful while sourcing financial advisors to avoid such pitfalls.

INTEGRATING RISK MANAGEMENT IN BUSINESS PROCESSES

Joshua Kibirige
AML Risk Manager,
National Social Security Fund

One of the barriers to effective risk management is to look at it as a separate process to be managed. Many organizations establish a risk management department and hope that all risks will be managed within the risk department. Risk is not a separate element from business activities, but part and parcel of them. Therefore, risk management needs to be integrated with business activities.

According to GRC 20/20 research, integrating risk management across the business is key to achieving an agile risk maturity stage, which requires understanding risk and compliance in the context of performance activities and objectives. It also involves having a consistent core risk and resilient processes across the organization.

The phrase "integrated risk management" was first coined by Gartner in 2017, in response to a more complex risk landscape, which organizations face.

Integrating risk management in all business processes is, however, still a challenge to many institutions. In many organizations, risk management activities are left to a particular business unit, staff, or department; such an arrangement cannot effectively manage the risks which the organization faces.

Organizations face a broad range of risks, which need to be effectively managed as a matter of routine, to avoid surprises. The risk management process should, therefore, be integrated into all business processes of the organization to ensure timely identification and mitigation of potential risks. Integrating risk management in all business processes can be achieved by:

Setting a risk appetite

The process of integrating risk management into all business processes should start with having an enterprise–wide risk appetite, which defines the nature and amount of risk the organization is willing to accept in pursuit of its objectives.

This helps to provide a link between the set strategy and the actual performance realized by the organization, because, for every key decision, the organization has to determine whether it is within its risk appetite. The risk appetite provides the needed balance between creating and protecting value of the organization.

Ensuring risk assessments are done before implementing any key decision or project.

Integrating risk management in business processes is also achieved by conducting risk assessments before implementing key decisions within the organization. This helps to figure out what could possibly go wrong and devise ways and means to minimize the likelihood and/or impact of materialization of the risk.

Implementation of key decisions without adequate or any risk assessments could lead to significant financial losses to the organization. For instance, the Reuters news agency in January 2012 revealed that Hewlett–Packard management lost about USD8.8 billion when it bought an information management software, company Autonomy, in 2011 for 11.6 billion dollars and wrote off 80 percent of the purchase price a year later.

Such a loss, resulting from overpaying for the acquisition, can be prevented if risk management is integrated in the process of decision–making and project management.

Control self–assessment (CSA)

CSA is a process by which process owners evaluate the adequacy and effectiveness of the controls in relation to the process risks in their jurisdictions. CSA can help to achieve risk integration by engaging employees in the process of identifying, analyzing, evaluating and mitigating risks. Involving process owners in assessing risks and controls builds a positive culture of risk management at every level within the organization.

Rewarding good risk–taking and punishing reckless risk–taking

Good risk taking refers to business activities done within the limits of the risk appetite, and can result in a profit for the organizations, while reckless risk–taking includes any activity done outside the organizations' risk appetite, whether it results into a profit or loss for the company.

To achieve risk integration, organizations need to establish a mechanism of rewarding good risk–taking and punishing reckless risk–taking. For example, in the case of Barings Bank, from 1992, Leeson made unauthorized speculative trades which first made large profits for Barings: and he earned a bonus of £130,000 on his salary of £50,000 for that year. The trader continued to place unauthorized trades which later resulted into losses for the organization.

Assign responsibility and accountability for risk management across the organization.

Assigning accountability for risk management can help to achieve risk integration by ensuring that all staff take responsibility for their own failures or successes, for activities and decisions undertaken in line with the defined risk management principles.

Risk accountability and responsibility means staff understanding of a risk, establishing controls or processes to manage the risk, reporting on the performance of those controls and processes, and ultimately guiding the business's response to that particular risk.

Introduce KPIs for risk management as part of the organizational performance appraisal framework.

Organizations can achieve risk integration by establishing key performance indicators (KPIs) as part of the organization's performance appraisal framework for all staff, e.g., number of staff turnover, number of system breakdowns, number of errors made in processing tasks and turnaround time for resolving customer complaints, etc. Such KPIs are based on the risks the organization expects to experience within the financial year and create a plan to mitigate them. Staff are then evaluated at the end of the financial year according to how well they implemented the controls to mitigate the identified risks.

Risk training and sensitization

Risk training can help to achieve effective risk integration by improving the ability of staff to identify and to respond to risk.

An effective risk sensitization programme helps to increase awareness of risk and risk management and empowers staff with the knowledge to identify and mitigate risk throughout the organization. For example, staff may start to notice gaps in processes that can result into losses and raise red flags to their managers or supervisors.

In conclusion, while risk management plays a critical role in the success of any organization, its benefits may not be realized if it is not integrated into all business processes. Such an integration can be achieved by undertaking the above–mentioned interventions.

THE IMPORTANCE OF A POSITIVE RISK CULTURE FOR THE 21ST CENTURY ORGANIZATIONS

Sospeter Thiga
Group Head, Risk & Quality Assurance,
CPF Financial Services, Nairobi Kenya

The 21st century organizations operate in a volatile, uncertain, complex, and dynamic world. Without a strong risk management culture, organizations are most certainly bound to fail. Culture has been defined as the way people get things done, in other words, their common habits.

Each organization has its way of getting things done, some organizations are fast and efficient while others are bureaucratic and inefficient. Culture is built in an organization over a long period of time and is often driven from the top.

Organization culture in turn influences risk culture, which is defined as the way organizations perceive risk and how they practice risk management. A positive organizational culture is likely to lead to a positive risk culture, and this is important because:

i) A positive risk culture will help an organization save on costs related to making wrong decisions, litigation from customers, correcting or recalling products, to mention a few. We have often seen organizations undergo through a painful process of rectifying their shortcomings for issues that could have easily been corrected through a robust risk culture. For instance, Volkswagen remains top of the mind following its massive recall in 2015 and the huge penalties from its regulator for the emissions scandal.

ii) An organization with a positive risk culture can avoid negative surprises by being ready for various scenarios. Covid–19 caught many organizations unprepared, however, organizations with a strong risk culture had probably mapped out the risk of pandemics and made plans to manage it through such measures as setting up and testing a business continuity management program.

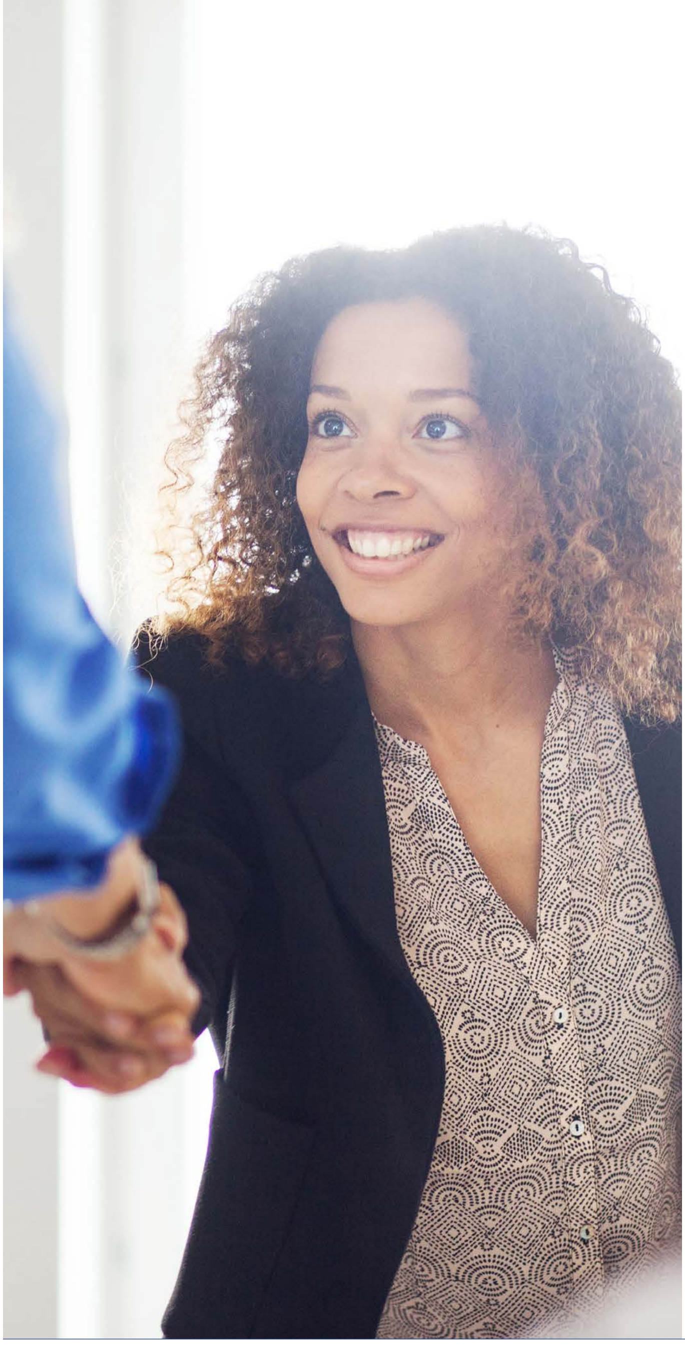
iii) A positive risk culture can help the organization to safeguard its reputation against malicious attacks. Managing the risk of customer dissatisfaction, especially in today’s complex world, where social media tends to exaggerate and accelerate negative news, is important. Once gaps have been identified, an organization should work to ensure that no customer goes away dissatisfied.

The recent run–on Chase Bank Kenya is testament to how quickly social media can bring an organization to its knees. According to the article, ‘The collapse of a major bank says a lot about the rise of Kenya’s powerful social media space’, by Nanjala Nyabola, It all started through a rumor on numerous WhatsApp groups that one of the Kenya’s best known mid–sized banks, Chase Bank,was in trouble, then to Twitter. Many depositors with the bank had to withdraw their savings, which caused liquidity challenges for the bank. In a space of four days, after a social media post, on Apr. 7, 2016, Chase Bank was under receivership—taken over by the Central Bank.

iv) A strong risk culture also helps organizations take advantage of opportunities and create value for the stakeholders. They say, "every cloud has a silver lining"; during Covid–19, organizations such as Amazon in the US thrived. For instance, according to an article titled: 'How Amazon managed the coronavirus crisis and came out stronger', by Annie Palmer, Amazon spent billions on safety measures for workers and internal testing initiatives. This permitted the company to keep hiring, increasing its staff head count by 34% in a space of three months (April to June 30 2020), in order to fulfill customer orders. This led to surge in sales of one of its product lines, the cough and cold medicine, by 862%!

V) The process of risk management often discovers opportunities that should be exploited for the benefit of the organization. For instance, while assessing the risks associated with entering a new market, the organization may discover untapped customer segments or favorable market conditions that present an opportunity for growth. Best of all, organizations with a strong risk culture have greater resilience.

Resilience has been described by Professor David Denyer, as the ability of an organization to not only bounce back but also bounce forward after extreme events. A positive risk culture promotes resilience through proactive identification and mitigation of rare risks (black swans), which could have severe consequences.



Risk culture can be improved through:

Setting the right tone at the top.

What top management does or says and how they behave towards risk and risk management, informs the rest of the organization how risk management practices should be in that organization. The board, CEO and Senior Management should be cognizant of this fact and be deliberate about passing on the right cues to the rest of the organization.

Right cues include emphasizing open and transparent communication, recognizing and rewarding risk management efforts, leading by example, fostering collaboration and cross–functional engagement, aligning risk management with strategic objectives, encouraging proactive risk management, teamwork, ethical behavior, and responsiveness to customers.

The Board, CEO and Senior Management should also embrace a positive risk management attitude by empowering and resourcing the risk function and its activities.

Establishing risk management structures and frameworks.

According to ISO 31000, risk management should be structured and comprehensive. As such, organizations should set up a dedicated function, which is well resourced, coordinate risk management activities, put in place a risk management policy, and train staff and management on risk management. The board should require risk assessment for all major initiatives that are proposed by management and regular risk reports during their meetings.

Appointment of risk champions.

The risk management function is ideally a coordinating function. Suffice to say that they cannot be subject matter experts in every discipline. The appointment of risk champions has proved a useful practice over time, in addressing this gap.

Additionally, risk champions help to domesticate risk within the departments they work in, thereby, allowing for greater ownership of the risk management process. I have found it useful to also have a sponsor at the board level.

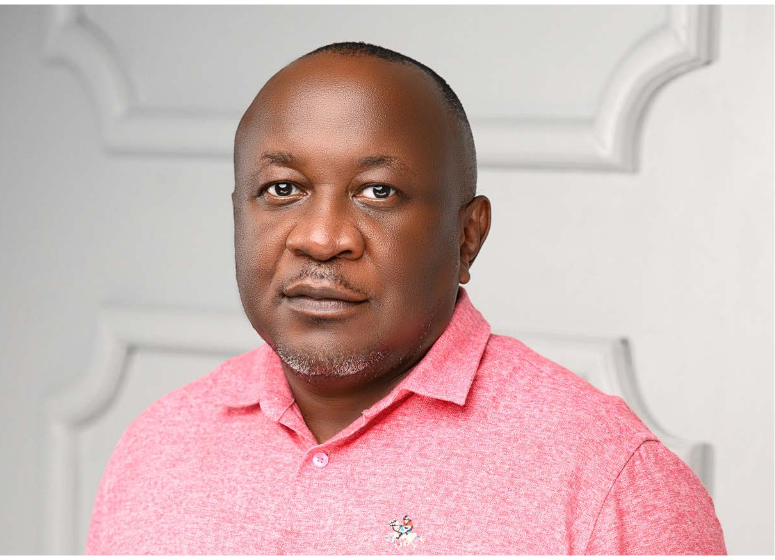
A sponsor should be well trained and have a clear understanding of risk management. The sponsor drives discussions on risk at the board level, which helps establish a strong culture at this level.

These initiatives go a long way in establishing a positive and strong risk culture.

Conclusion

Professor Peter Drucker famously said, "culture eats strategy for breakfast", he could not have summarized my thoughts better. A negative culture will eventually cannibalize anything in its path, including risk management, if not well managed. It is important for organizations to endeavor to achieve a positive risk culture if they hope to survive and thrive in the 21st century.

SETTING THE RIGHT TONE ON RISK MANAGEMENT



Edward Senyonjo
Chief Risk Officer,
National Social Security Fund

Organizations are structured like a human body; they have top management, middle management, and the junior level, which can be likened to the head, the torso, and the legs of a human being. The only difference is that, unlike the human body, at different levels of the organization, that is, top management, middle management and the lower level, there is a brain which makes decisions.

Nonetheless, major and impactful decisions are made at the top management level, and the rest of the organization just implements the decisions made by top management, just as the legs and hands of a human being implement what the brain tells them.

Therefore, the decisions or actions of top management have got a profound impact on the rest of the organization. Top management determines the direction, strategy, vision, mission, and the culture of the organization. It goes without saying that the attitudes and actions of top management greatly influence the risk culture of the organization. In other words, top management sets the tone for risk management. The board sets the tune, management sings the tune, and the rest of the employees dance to the tune. A right tone from the top is key in developing appropriate risk management practices and culture in the organization.

One of the cardinal roles of the board is to ensure that risks facing the organization are comprehensively identified and effectively managed, so as to enable the organization to attain its objective. This is because risks affect the objectives of the organization.

Unfortunately, oftentimes, in many organizations, risk management is seen as an "obstacle" to organizational operations. Human nature is such that, when we plan to do something, we hope and wish the outcome will be positive. Even a robber wishes and hopes that the robbery will be successful! Usually, we do not give much thought to the question of "what can go wrong or what if this or that goes wrong?".

Therefore, because our human nature is more inclined to the positive side of things, any attempt to consider a possible negative outcome is usually met with resistance, and whoever stands on the side of caution, is seen as a "prophet of doom" or not a team player. Indeed, traditionally, speaking of what is likely to go wrong about a good idea, is considered a "curse" and discouraged, saying, "totukuba kisiraani", in Luganda; literally meaning, don't bring a bad omen on us.

It is not surprising that risk managers are not the most popular employees in many organizations because they speak about what other employees wouldn't want to hear, and yet it (risk) is a reality of life– risk is a constant, refer to the article, "Risk is another constant", in the sixth issue of The Risk Echo magazine. In many organizations risk managers are not referred to by their names, but by expressions such as "the risk guy, the risk man, etc.", which reflects the negative culture towards risk management in such organizations.

Secondly, due to the negative attitude towards risk management, the risk departments are usually under–resourced, in terms of budget, tools and personnel, and yet the risk department has the widest scope, since risk is

associated with every activity that the organization undertakes.

As mentioned above, it is top management that creates such a culture, and it is top management that can change such a culture. By setting the right tone, the board and executive management can play a major role in creating an appropriate risk management environment, which helps the organization to attain its objectives, by identifying, assessing, and recommending measures to address potential negative effects on the objectives.

According to Evelyn C. Bauman's article (2020), "in the risk–management context", tone from the top has two dimensions: (1) a top–down approach including top management communication of commitment and behavioral expectations with regard to risk management, and (2) encouragement of bottom–up communication and escalation of risk issues.

The tone from the top should be both in words and actions, as explained below:

a) Set a risk appetite

A risk appetite defines the nature and amount of risk the board is willing to accept in pursuit of organizational objectives. A risk appetite, therefore, acts as a boundary for decision–making since decisions have to be made within the risk appetite framework. A risk appetite also inculcates discipline and prudence in decision–making. For every key decision, the critical question to ask is that, is this within our risk appetite?

b) Empower risk managers.

Ensure that the risk department is well resourced in terms of skills, competencies, tools and finances, coupled with the board's full backing to implement enterprise risk management activities.

c) Reporting structure

Usually, major decisions are made at the board and executive levels, and this is where major risks emanate. It is, therefore, important that the person in charge of enterprise risk management sits at this level, such that he/she provides timely advice as regards to risks related to the decisions made, which have organization–wide implications. In other words, the officer in charge of enterprise risk management should be of appropriate seniority, preferably an executive (Chief Risk Officer– CRO), who reports to the Chief Executive Officer or an Executive Director. It would also be appropriate for the CRO to have a dotted line to a committee of the board in charge of risk management.

d) Policies and procedures

Ensure that risk management frameworks (policies, procedures and guidelines) are in place to guide risk management activities.

e) Monitoring and reporting risk

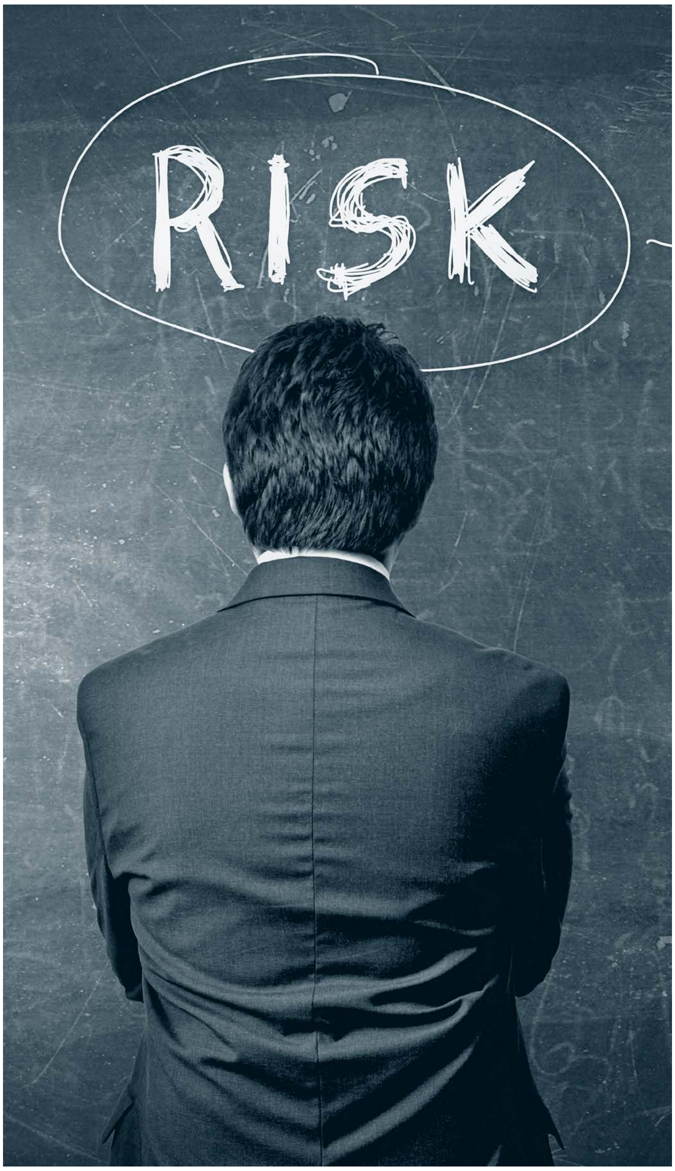
Provide a mechanism for the CRO to regularly monitor and report emerging risks and relevant mitigation measures to executive management, and the board through a board risk committee. The board can adopt the recommendations of the CRO and direct management to implement them.

f) New products, systems and processes.

The board should require a risk assessment report to accompany any request from management to introduce or make changes to existing systems, processes, procedures, products and facilities.

g) Performance measurement

Performance indicators for risk management, e.g., percentage of risk management recommendations implemented in time, percentage of effective controls, number of risk awareness programs attended, etc, should be incorporated in the organization's performance measurement framework.



h) Incident reporting

Provide a channel through which staff can report incidents as and when they happen. The reported incidents should be analyzed to identify the cause, assess the impact, and determine measures to prevent future occurrence of similar incidents. For those who prefer to report in confidence, a whistleblowing mechanism should be provided. This encourages staff to report cases of abuse of resources and misconduct without fear of retribution.

CONCLUSION

A positive tone from the top sets a stage for effective risk management, which enables the organization to attain its objectives. An organization with positive risk culture uses risk management frameworks and processes effectively to create and protect value. Effective risk management is a critical determinant of success of any organization.

IS YOUR SYSTEM DEVELOPMENT PROCESS A BOTTLENECK? SWITCH TO DevSecOps

Brian Nuwagaba Ludovic
Information Security Specialist,
National Social Security Fund.

One of the critical shortcomings of the traditional system development life cycle (SDLC) is its failure to incorporate the critical elements of security at the initial stages of development, which causes delays in the implementation of the project.

Phrases such as "IT security guys are showstoppers, enemies of progress, agile intolerant," to mention but a few, are oftentimes a manifestation of system users' frustration with the traditional software development life cycle.

These phrases are too common when it comes to software development projects in most organizations that still follow the traditional approach to software development. For the most part, I'd associate with such frustrations. Traditionally, software development has followed the conventional software development lifecycle approach (SDLC), which consists of primarily six phases:

Phase 1: Planning and requirements analysis

Like for all other projects, planning is required to determine the resource requirements, the project timeline, cost, quality control requirements, etc. Developers typically gather input from anticipated users of the system, both internal and external. Essentially, all the information gathered during this phase forms part of the building blocks for this project.

Phase 2: Requirements definition

Here, all the above requirements are then documented, and approvals are sought from the system users and other interested stakeholders. This culminates into the software requirements specification document.

Phase 3: Architectural design

The architectural team will then come up with an architectural design for the software to be developed. Multiple designs will usually be proposed and iterated through until a best fit-for-purpose design is agreed on by all interested parties.

Phase 4: Development

In this phase, the developers will begin to translate the defined requirements into actual code using any of their favourite programming languages. This is done within the confines of the agreed architectural design.

Phase 5: Testing and integration

Once the initial phase of development is done, the product/software will then need to be tested to ensure the functionality meets the stakeholder's requirements. In this phase, documentation relating to the product/software will also be developed and user training undertaken.
In most cases, it is at this point that the security teams are then called in, to ensure the organization's security requirements are met.

Phase 6: Deployment and maintenance

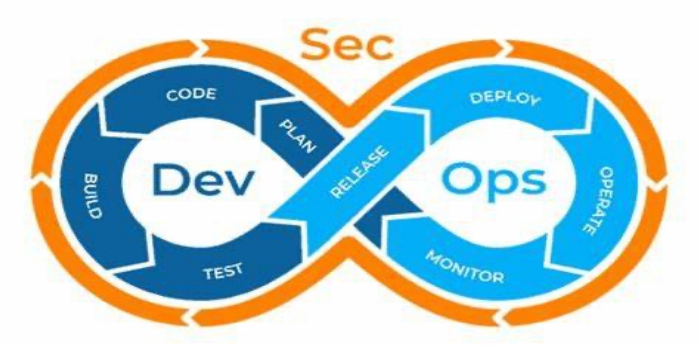
Once the teams are happy with the final product, it is then deployed into a live environment, wherein the customer can begin to use the software. As one may observe, the security teams are typically called in at the tail end of the entire process.

This creates one major drawback which is that, often serious security flaws will be picked up at this point, resulting in the teams going back to the drawing board. This derails the project significantly, causing financial loss to the organization.

Due to these shortcomings, the DevSecOps (Development, Security and Operations) was later developed. The history of DevSecOps dates to as far as 1976, where security attributes such as access control were recognized and embedded into the process.

Of course, at the time there were not many 'hackers' and so the maturity levels were still rather low. Today, it has evolved to having more security attributes such as vulnerability scans, attack monitoring, encryption etc.

In summary, DevSecOps is the integration of security at every phase of the SDLC process described above. The image below illustrates the typical process a product would go through under the DevSecOps approach.



Below we delve into how entities can practically embed this model into each phase of the SDLC process.

Phase 1: Planning and requirements analysis

The team composition becomes a critical factor here as you roll out the project. The team should have diverse skill sets. For example, whilst you would have the traditional systems and network administrators to handle the physical infrastructure, you would also need to have security specialists on the team to ensure that security requirements are identified and defined. This way, based on the OSI (Open Systems Interconnection) architectural model, your security requirements are covered at all layers.

An example of such a requirement could be to ensure that all user stories and features contain functional security constraints, such as “As a user, I should be able to view and edit my profile, but I should not be able to view or edit anyone else’s profile”.

Such functional security requirements are often overlooked by the DevOps teams until later when the security teams are involved, and yet lack of these subtle features could result into serious system compromises.

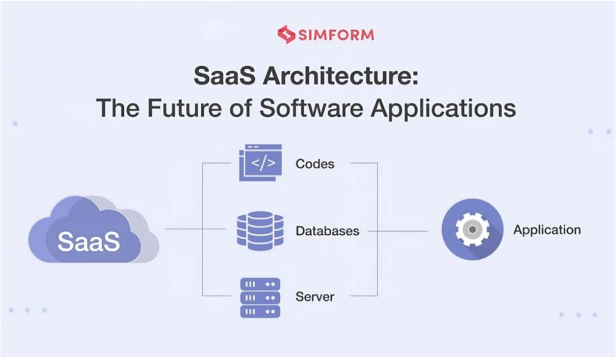
Phase 2: Security requirements definition

Like the SDLC process flow, security requirements definitions also need to be documented as well. Documentation relating to application data flows, components and trust boundaries needs to be reviewed and approvals sought. Having these documented, allows future teams to quickly assess an application’s security capabilities as well as any failed controls that need to be improved.

Phase 3: Architectural design

In this phase, the security teams would provide direction on what security capabilities to be embedded in the design to ensure the confidentiality, integrity, and availability requirements of the organization are met. Often threat modelling is performed to determine possible threats at each point of the design.

A simple cloud enterprise architectural diagram is shown below. This enables the security teams to have a “bird’s eye” view, and will often come in handy when a major security incident materializes.



(Ref: Pin on SAAS (simform.com))

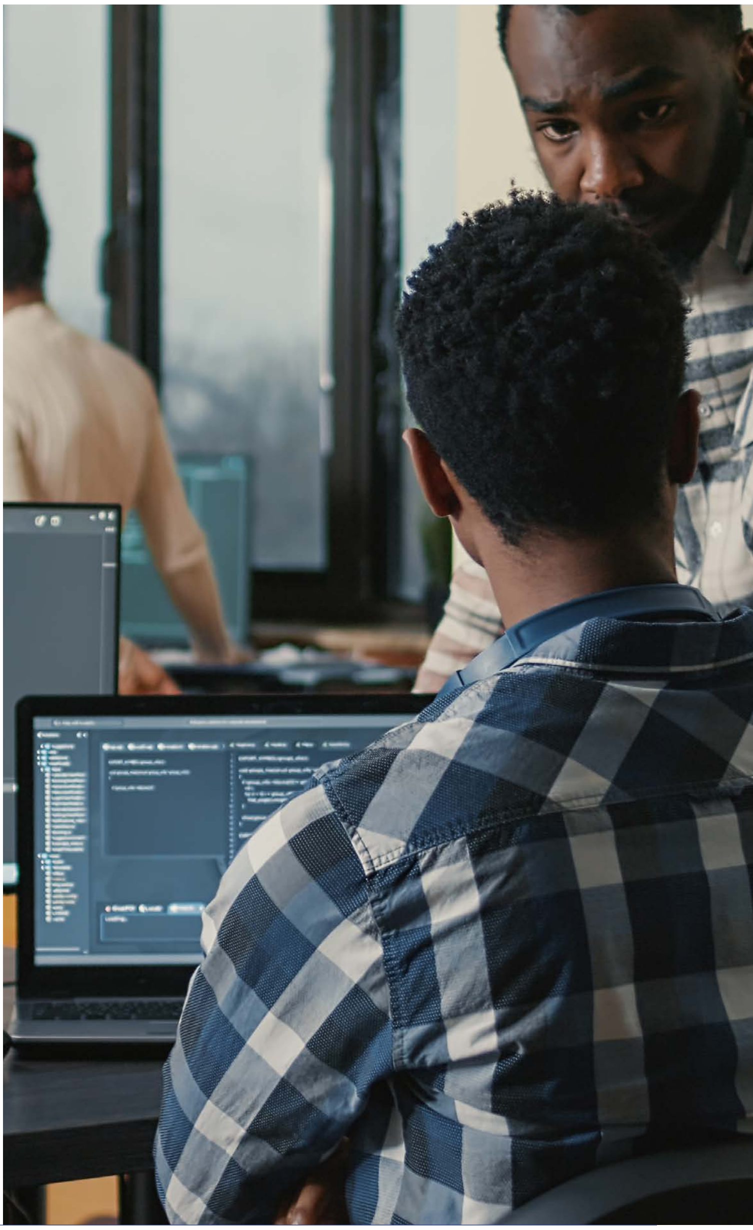
Phase 4: Development

At this point, security automation is done where continuous improvement/delivery (CI/CD) pipelines are developed to automate security and allow for shorter go–to–market time.
The idea now is to embed the security function at each point. Below is how one may approach this.

i. Development stage

Here, several Integrated Development Environment (IDE) security plugins can be used. These plugins would provide real–time feedback as the developer writes codes. For example, the plugin would warn a developer if he/she attempted to use known vulnerable code functions and make suggestions to more hardened alternatives.

For developers using version control systems like git, pre–commit hooks can also be run to check the quality of the code. For example, a simple check might be done to ensure credentials are not pushed with the code into the repository.
The developer would need to also reference the organization’s secure coding standards as they progress. Code peer reviews are equally important, as it allows a peer reviewer to pick up issues that could have been missed from the start.



ii. Commit stage:

Static code analysis tools can be used in this phase. Code scans are run against the code repository to pick up any issues and provide instant feedback for remediation. Dependency management tools also play a critical role in this stage. These tools will map out all your 3rd party libraries / packages on which your application depends. Having this information allows you to quickly know which libraries need updating or have known security vulnerabilities. This also helps an organization track licensing status for all these 3rd party libraries / packages used.

Phase 5: Testing and Integration

The goal in this stage is to have a comprehensive check of both the application and infrastructure. For example, one might want to ensure that the provisioned server does not have unintended publicly available ports. If you have a cloud environment, this task is simplified by services such as Infrastructure–as–code, wherein a server can be deployed already hardened. This build in your pipeline would fail if say, a server was deployed with below–the–line minimum security requirements as defined in your organization’s standards.

Dynamic code scanning tools are then used at this stage. Unlike the static code analysis tools that looked at code, these tools now scan the application interactively and often help with picking up issues that can be remediated. This scan can also be automated by spinning up a container with your respective scanning tool.

Security acceptance testing can then be done by the security team. Test case scenarios earlier discussed from the threat modelling exercise are then executed to ascertain that, indeed, the application did handle such threats. These could range from tests for Structured Query Language (SQL) injections attacks to cross–authorization issues.

Phase 6: Deployment and maintenance

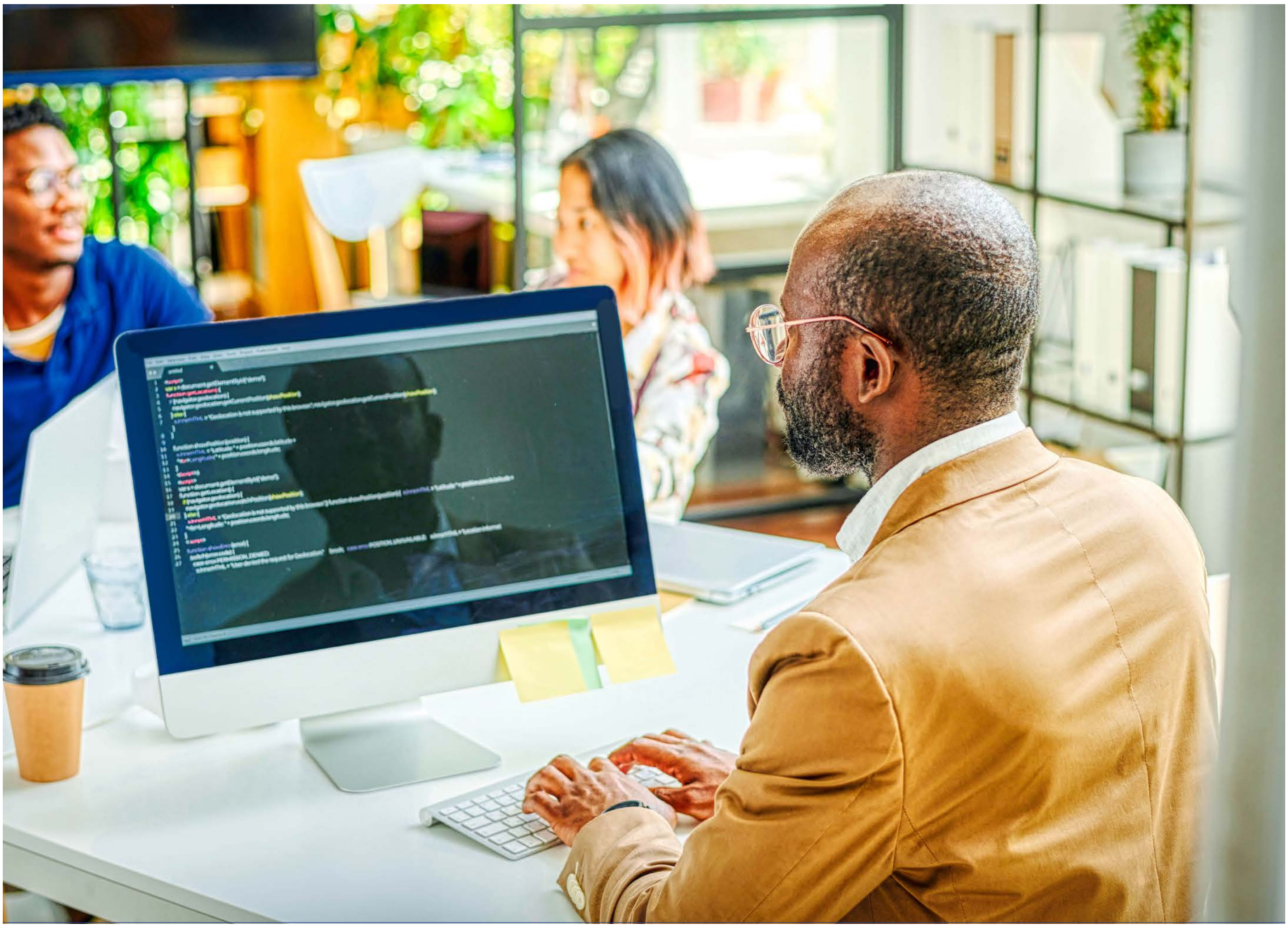
Configuration checks are done at this stage. If you are in a cloud environment, then this task too can be automated through the various configuration check tools provided by all major cloud providers. As a best practice, only the CI/CD pipeline should have access to the production subscription. In other words, all server and application deployments are done through the pipeline.

Based on the criticality of the application, a penetration test may also need to be carried out before rolling out to customers. Now, I know this may not sit well with the agile work culture we all want to lean towards. But this exercise often provides valuable feedback on potentially exploitable issues that could have been missed, and is usually worth the wait in this case.

Continuous monitoring is essential here. This could be lessons learned by the teams and feeding back into the pipeline to improve and further secure the final product. Organizations can also sign up for threat intelligence feeds to keep up to date with ongoing attacks. Recurring vulnerability assessments need to be done at this stage as well. This could be as simple as running a weekly scan on your application to pick up any vulnerabilities that materialize. Remember the application might be using 3rd party libraries for which updates need to be applied as well.

Conclusion

DevSecOps requires a collaborative work culture, where everybody understands that security is a shared responsibility. Having security teams involved right from the word go, significantly cuts back go–to–market time and product cost.



SAY GOODBYE TO CLUTTER...
...AND HELLO TO A PAPERLESS OFFICE

PUZZLE ISSUE NO. 7

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

ACROSS

1. Process of doing something,6

2. Responsible for various administrative duties that directly support an individual or an office, abbr.2

3. Skill and sensitivity in dealing with others or with difficult issues,4

4. Extending directly upwards from,4

5. Created in order to facilitate greater sharing of information, abbr.3

6. An executive who is tasked with the identification, analysis, and mitigation of events that could threaten a company,abbr.3

7. Before noon,2

8. With no part left out,6

9. A designation for professionals who are actively involved in risk management, strategic planning, corporate governance, project management, controls, auditing, and business consultancy, abbr.4

10. Buildings used for musical performances (especially in ancient Greece or Rome),4

11. A figure companies or analysts use to measure risk,abbr.3

12. An international organization founded in 1945,abbr.2

13. Part of the electromagnetic spectrum, abbr.2

14. Federal agency responsible for enforcing laws and regulations governing narcotics and controlled substances,abbr.3

15. A special branch of the police force that prevents terrorist activities in the country,abbr.3

16. A large village in Derbyshire, England,8

17. Undersurface of a person's foot,4

18. Most common form of arthritis. Some people call it degenerative joint disease,abbr.2

19. Opposite of southwest, abbr.

20. Shoot at someone from a hiding place, especially accurately and at long range (noun),4

21. Positive declaration intended to give confidence; a promise,9

DOWN

1. Persons or entities that attempt to access, extract, insert, reveal, influence, delete, or disclose another party's data without prior authorization or permission,9

2. Extracurricular school activity, abbr.2

7. Document given to a customer who has returned goods, which can be offset against future purchases,abbr.2

8. Unit for measuring the width of printed matter,2

12. Universities Admission Index,abbr.3

15. Another time; once more,5

20. High or higher in rank or status, abbr.2

22. Not showing or feeling nervousness, anger, or other strong emotions, (Comparative adj.),6

23. Enables data to be transferred between applications and devices on a network, abbr.3

24. A broad professional category covering functions including building communications networks, safeguarding data, and troubleshooting abbr.2

25. Industry–leading antivirus and security software for PC, Mac, or mobile devices,6

26. Amounts overdue; money owed and should have been paid earlier,7

27. Not valid or legally binding,4

28. Companies that own, operate, or finance income–generating real estates, abbr.5

29. Statements intentionally phrased to require ingenuity in ascertaining their answers or meanings,7

30. A metropolis in central Netherlands,3

31. Atoms bearing one or more positive or negative electrical charges,4

32. A combining form meaning "nine, ninth," used in the formation of compound words,4

33. Payment made to an expert or a professional body in exchange for advice or services,3

34. A microcomputer designed for use by one person at a time,abbr.2

SOLUTION TO ISSUE NO.6

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