

www.oaoinvestments.com

AFRICA

OAO TECHMAG

ISSUE 1 NOVEMBER 2022

THE FINANCIAL
IMPACT
OF A CYBERATTACK

BUSI MATHE

CYBERSECURITY:
THE ROLE OF
THE BOARD

ZAMOKUHLE
AJA-OKORIE

HOW TO RECOVER
FOLLOWING A
CYBERATTACK

SWEDISH AI
PARTNERSHIP

ADV PANSY TLAKULA

THE INFORMATION
REGULATOR ON DATA
VULNERABILITY

The
CYBERSECURITY *Issue*





ACCELERATING THE ADOPTION
OF NEW TECHNOLOGIES IN AFRICA



WHAT
DRIVES US?
YOUR
SUCCESS!

OAO
TECHNOLOGY

www.oaoinvestments.com/oao-tech

C ontents

COVER

Busi Mathe

8 Cybersecurity: the Role of the Board

12 **Zamokuhle Aja-Okorie**
Cyberattack! What Next

14 The Financial Impact of a Cyberattack

16 **Adv Pansy Tlakula**
Information Regulator



BUSINESS

20 Digital Brand Protection
Strategy - Why You Need One

27 Effective Communication in
the Event of a Cyberattack

25 The Rising Threat of Cyber
Attacks on African Fintechs

The Fight Against Phone
28 **Hacking**
Sim Card Protection



BUSINESS

39 **OAo Investments Announces Partnership With Swedish AI Fund**

WOMEN IN TECHNOLOGY

32 **Debbie Botha**
How To Keep Women in Tech

36 **Beat Imposter Syndrome**

38 **Betty Mbithi**
Feature



32

LEGAL

22 **Professor Sizwe Snail ka Mtuze**
CyberCrime Act



IN EVERY ISSUE

- 7** Editor's Letter
- 8** Publishing Panel
- 11** Subscription & Advertising



Cover Photography by
LONGTERM UTOPIAN MEDIA



E

ditor's Note

I'm excited to announce the launch edition of OAO Tech Mag. The first issue which was produced over a few months with missed deadlines due to several challenges as a launch issue, and coming from a relatively new business in the market, did not come without stress! But I'm happy to say that through hard work and dedication we made it happen. OAO stands for One Africa Odyssey with a vision to accelerate the adoption of new technologies on the continent. The Covid-19 pandemic forcefully catapulted the transition onto digital platforms, allowing for global awareness and opportunities rooted in Africa. Our first edition focuses on Cyber Security geared towards the executive suites, the knowledge they require and the role they play in the decision-making of their company's cyber security.

This edition provides insight into various aspects of Cyber Security which include the latest information and emerging trends in the industry. It highlights cyber security as being an "everyone's issue" and not the sole responsibility of the Tech department/person. It also addresses the matter of Women in AI and how we can entice them to stay past a certain point on the career ladder.

Starting a brand-new magazine is inspiring yet exhausting. The unique challenges we faced could be shared in a book that we will leave unpublished for obvious reasons once you've perused this edition. I hope that this edition of OAO Tech Mag will boost your confidence in us, and help you find your path to a safer, more secure cyber experience. See you in the next edition where we spotlight Artificial Intelligence.

Mariam

TALK TO ME...

 @OAO-TechMag

 OAO Investments

 techmag@oaoinvestments.com

OAOTechMAG

Content Director

ZAMOKUHLE AJA-OKORIE

Editor

MARIAM HOOSEN

Contributors

BETTY MBITHI

BUSISIWE MATHE

DEBBIE BOTHA

FAATIMA KHOLVADIA

LANBE OGUNGBE

OBINNA AJA-OKORIE

ONYINYE OKONKWO

ADVOCATE PANSY TLAKULA

PROFESSOR SIZWE SNAIL KA MTUZE

Digital Content Producer

APHIWE SABELA

Art Director

ZAMOKUHLE AJA-OKORIE

Graphic Designers

ERIN VAN ASWEGEN

ENQUIRIES: info@oaoinvestments.com

EXECUTIVE TEAM

Founder & MD ZAMOKUHLE AJA-OKORIE Chief Marketing Officer MARIAM HOOSEN

The trademark OAO TechMag is the property of OAO Investments (Pty) Ltd © 2012. All rights reserved. No material may be reproduced in part or in whole without written consent from the copyright holders. OAO Publishing does not accept responsibility for damage to or loss of freelance material submitted for publication. All financial advice published in the magazine has been prepared without taking into account the financial situation, objectives or needs of the reader. OAO TechMag, OAO Investments and its employees do not hold any responsibility for any losses and or injury incurred by anyone acting on the information provided in this magazine. All opinions expressed are held solely by the contributors and are not endorsed by OAO TechMag.

BUSINESS MATTER

Cybersecurity & *THE ROLE OF THE BOARD*

Cyber risk remains among the top risks facing business organisations today. The World Economic Forum's Global Risk Report 2021 lists cybersecurity failure as a top "clear and present danger" and critical global threat. As with any major enterprise issue, it is important for the board of directors and leadership to set the tone at the top and define how their organisations must address cybersecurity. The board needs to understand cyber risk, and its role in governing this threat, to perform its oversight function effectively. It continues to be important for members of the board of directors to increase their knowledge of how to address cybersecurity within their organisations.

The Board not only looks at the company's financial systems and controls but is also duty-bound to oversee its overall cybersecurity management, including appropriate risk mitigation strategies, systems, processes, and controls. From a governance perspective, one of the most important priorities for the board is to verify that management has a clear perspective when it comes to how the business will be affected and has the appropriate skills, resources, and approaches in place to minimise the likelihood of a cyberattack and mitigate any damages that may occur.

The following are a few concepts that boards need to have or understand about cybersecurity:

1. Cybersecurity goes beyond protecting data.

To oversee cybersecurity in today's business environment requires a more holistic

approach. This involves considering digital and connected systems that control the organisation's information supply chains, production processes (such as the remote management of equipment) and the management of a digitally connected remote workforce. Directors need a general understanding of the security ecosystem, and relationships within, to adequately address risk.

2. Cybersecurity is an organisational problem, not just an IT problem.

Cybersecurity requires awareness and action from all members of the organisation to recognise anomalies, alert leaders, and ultimately mitigate risks. Leaders set the tone for prioritising this kind of culture, but they also reinforce and personify the values and beliefs for action. The Board has a role in this; by asking questions about cybersecurity, directors imply that it is an important topic for them, and that sends the message that it needs to be a priority for corporate executives.

3. Boards should focus on risk, reputation, and business continuity.

Cyber-professionals focus on the tactical level: how to address the technical, operational, and organisational aspects of cybersecurity. Directors do not require the same technical knowledge as these professionals. They must look at the issue from a macro perspective and focus on the impacts on risk, reputation, and business continuity. By focusing on common goals: keeping the organisation safe and operational continuity, the gap between the Board's role and the cybersecurity professionals' role can be narrowed.

“BOARDS CAN'T SHY AWAY FROM THEIR CYBERSECURITY GOVERNANCE RESPONSIBILITIES. AS THE MOST VALUABLE ASSETS OF ORGANISATIONS ARE DIGITISED, STAKEHOLDERS EXPECT THE ORGANISATION TO EMPLOY ALL POSSIBLE MEASURES TO PROTECT ITSELF AGAINST THE PERILOUS CYBERSECURITY LANDSCAPE.

4. Boards need to be engaged when it comes to cybersecurity oversight.

It's not the board's role to write and draft the organisation's cybersecurity plan. However, their role is to ensure that there is an actionable plan. There are many frameworks available to help an organization with their cybersecurity strategy (NIST, ISO, ICS etc.)

Below is a list of questions that will help boards understand how cybersecurity is being managed in the organisation:

1. What are our “crown jewels” or most critical assets — and how are we protecting them?

The board must make sure the organisation's most important assets are secure at the highest reasonable level. Is that your customer data, your systems and operational processes, or your company IP? Asking what is being protected and what needs to be protected is an important first step. If there is no agreement on what to protect, the rest of the cybersecurity strategy is subject to debate, dispute, or uncertainty.

2. What are the layers of protection we have put in place?

Boards don't need to make the decision on how to implement the defensive strategies required by the organisation. But they need to be made aware of what these are, as well as how effective they will be in protecting the company.

3. How do we know if we've been breached? How do we detect a data breach?

Part of the board's fiduciary duty is to ensure that the organisation has both protection and detection capabilities. Since majority of breaches are not detected immediately after they occur, the board must make sure it knows how a breach is detected and agree with the risk level resulting from this approach.

4. What are our response plans in the event of an incident?

Although the board will not likely be directly involved in the creation of a response plan, it's part of their responsibility to ensure there is one. This plan should involve answers to the following questions:

- ? What is the role of executives and leaders in the response plan
- ? What is the communications plan
- ? Who is responsible for alerting authorities
- ? Which authorities are alerted
- ? Who talks to the press
- ? Who will manage client and media concerns

Having a plan is critical to responding appropriately.

5. What is the board's role in the event of cyber-incidents?

It is important for the board to know what their role will be in the event of a cybersecurity breach. The board should consider conducting “fire drills” and tabletop exercises so they know what to do when a cyber-incident takes place. The board should also consider the following:

- ? Should the decision to pay out a ransom in a ransomware attack fall on the board
- ? What decisions should be delegated to management
- ? Should the board be accessible to customers?
- ? Should they meet with top organisation leaders for hands-on, agile decision-making

6. What is our business recovery plans in the event of a cyber incident?

It is important for the board to know who “owns” business recovery, whether there is a plan for how to make it happen, and if it has been tested with a cyber incident in mind?

7. Is our cybersecurity investment enough?

You can't invest enough to be 100% secure. But since a budget must be set, it is crucial that companies guarantee they have an excellent security team with the appropriate expertise to tackle technical problems and understand vulnerabilities inside the core critical functions of the business. By doing that, the company will be better prepared to allocate investment where it is most needed. Organisations should evaluate their level of protection and their risk tolerance before they engage in new investments. Two ways to do this are through simulations of cyber-attacks and from penetration/vulnerability tests. These actions expose vulnerabilities, enable actions to minimize potential damage based on priority, risk exposure and budget, and ultimately ensure appropriate investment of time, money, and resources.

Boards can't shy away from their cybersecurity governance responsibilities. As the most valuable assets of organisations are digitised, stakeholders expect the organisation to employ all possible measures to protect itself against the perilous cybersecurity landscape. This requires that the board asks the right questions, so cyber-priorities and plans can be laid out effectively.

Busisiwe is a seasoned business leader, who has experience in digital transformation, cybersecurity & data privacy. She is the Chief Executive Officer of Orirori Consulting and an Independent non-executive director at Famous Brands. She has worked across multiple industries/sectors assisting multinational organisations in understanding, managing & improving their cybersecurity & data privacy risks and issues by applying a business lens to these. Busisiwe is a qualified chartered accountant.

S

ubscriptions & Advertising



SUBSCRIBE

to *OAOTechMag*. Enjoy every issue delivered to you.

For subscriptions:

Scan the QR code or

Call +27 87 265 5406 Monday-Thursday
9am-4pm CAT

Email publishing@oaoinvestments.com

or subscribe online at

www.oaoinvestments.com/publishing



ADVERTISING

Looking to expand your footprint to our stakeholders? Place your brand in

OAOTechMag

For advertising:

Contact advertising@oaoinvestments.com

View our media kit

www.oaoinvestments.com/oaotech/oaotechmag/

ZAMOKUHLE AJA-OKORIE

CYBER ATTACK

What next?

South Africa ranks third in the world for cybercrimes costing approximately R2.2-billion annually. Throughout the globe, cybercriminals find new ways to target organisations. Regardless of the size of your business no network is impenetrable. Organisations can improve their cyber security position by remediating identified gaps and by establishing continual process improvement.

If your business has fallen victim to a data breach, consider the following steps:

Step 1: Isolate And Contain The Breach

Start by determining the compromised server. Identify and mitigate the vulnerabilities used to illegally access your network by isolating the affected endpoints and servers to ensure that other servers or devices won't be infected. Preserving the evidence will be key in accessing how the breach occurred and the responsible party.

Step 2: Seek Professional Help

Seek the services of IT security specialists. Remedying the situation in-house may be inefficient and potentially inadequate; a third-party audit is strongly advised. They will find other vulnerabilities facing your organisation and offer remedies to patching them.

Step 3: Alert Authorities

Report the incident to law enforcement authorities and your local African regulator as soon as possible. If you operate internationally notify the affected country's data regulator. Internationally companies are liable to report security data breaches and incidents. Companies can attract massive penalties from regulatory agencies should they fail to report the incident or report it late. Bookings.com was fined €475,000 for reporting a data breach 22 days after the attack.

“

WITH THE INDUSTRIALISATION OF CYBERCRIME, IT HAS BECOME A GLOBAL BUSINESS THAT GENERATES MORE REVENUE THAN THE DRUG TRADE TODAY. WEAPONISED CYBER THREATS CONTINUE TO ADVANCE AND FURTHER CRIPPLE GLOBAL COMMERCE.

MALICIOUS ACTORS HAVE CLEANED THEIR ACTS AND RUN SOPHISTICATED OPERATIONS. THEY PENETRATE SYSTEMS LOOKING FOR VULNERABLE INFRASTRUCTURE AND THEN THEY ATTACK. SO WHAT SHOULD YOU DO WHEN THEY ATTACK?

Step 4: Inform Clients

Reputational damage occurs when organisations fail to meet their clients' expectations. By maximising transparency and notifying your clients immediately after the breach, you create a sense of trust in your organisation. It shows commitment on your part to protecting your stakeholders. They too can take the necessary measures to protect themselves, their families and their organisations.

Step 5: Deploy Security Solutions

Come up with a set of efficient remedial measures to boost security and deal with potential cyber-attacks in the future. Use a layered security approach to your IT systems. Develop an in-depth defence strategy and deploy a series of different combined defences (firewalls, malware scanners, intrusion detection systems, data encryption and integrity auditing solutions). The strategy will effectively close the gaps that are created by relying on a singular security solution.

Step 6: Compile A Report

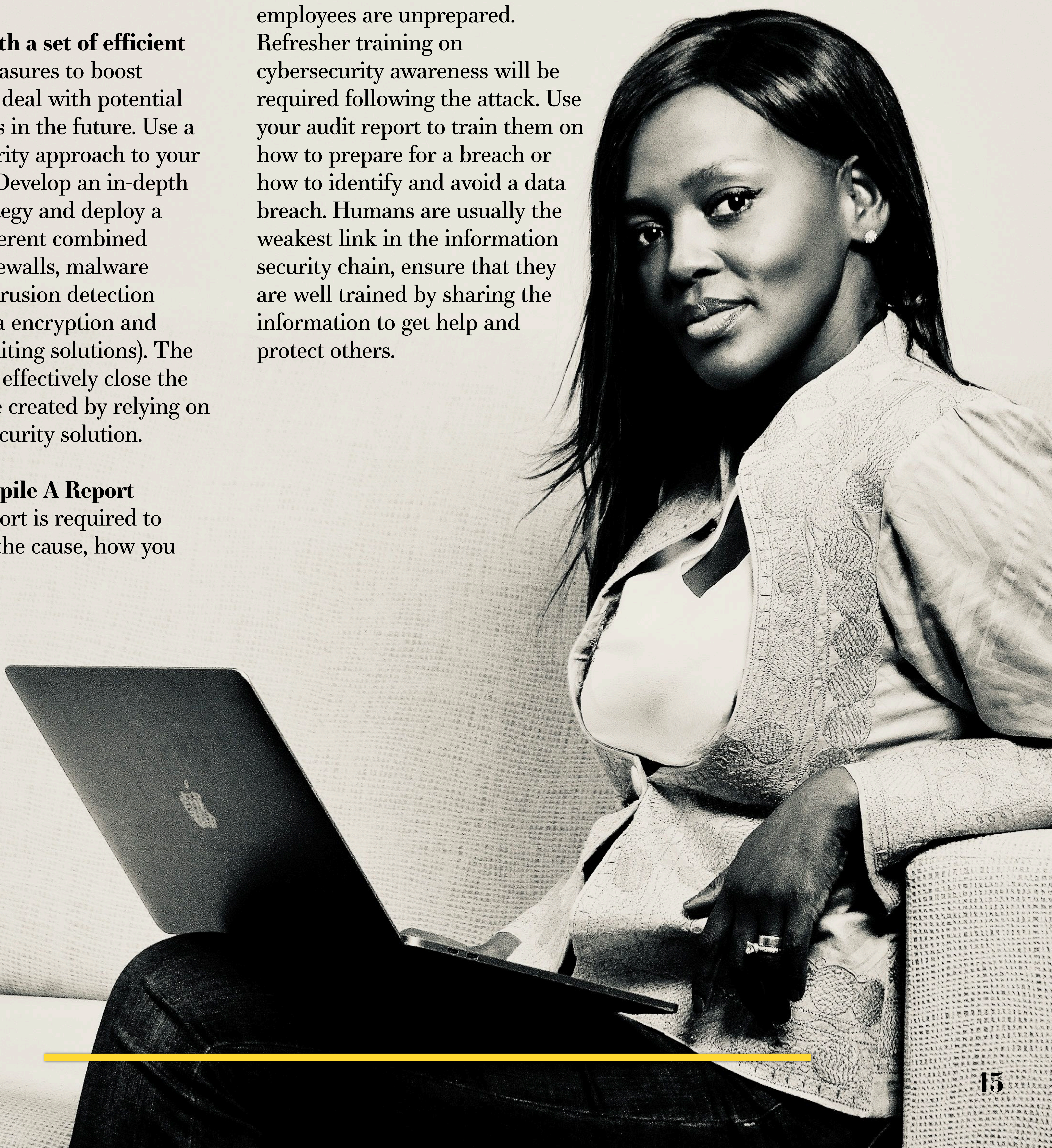
An audit report is required to understand the cause, how you

recovered, lessons learned and mitigate future attacks. It provides a way to encourage employee participation in cyber security awareness and prevention. Lessons gained from the report can be used for comparisons both within and between organisations and industries.

Step 7: Refresher Training

As employees are the first line of defence against cyber-attacks, they should be aware of your business policies regarding data breaches. The most carefully calibrated strategy falls short if your employees are unprepared. Refresher training on cybersecurity awareness will be required following the attack. Use your audit report to train them on how to prepare for a breach or how to identify and avoid a data breach. Humans are usually the weakest link in the information security chain, ensure that they are well trained by sharing the information to get help and protect others.

Due to the nature of business operations reliance on information technology, more so than ever as a result of the COVID 19 pandemic, cyber-attacks are inevitable. These are the consequences of operating in an increasingly connected digital world. To meet the challenges posed by a data breach your business will have to react in an agile and decisive way. It can be a stressful period, but if you take the necessary steps your business will build resilience to navigate future possible attacks.



FAATIMA KHOLVADIA

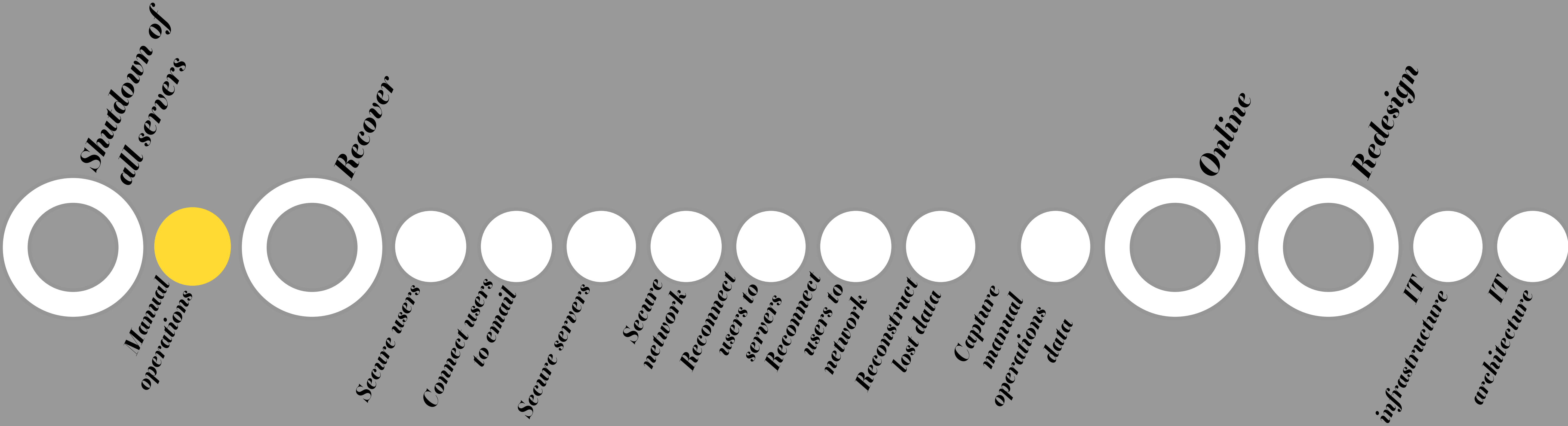
FINANCIAL IMPACT

of a cyberattack: *a framework*



The rapid spread of the coronavirus lead to Governments across the world implementing lockdowns and restricting movement, created a new normal of digital dependency and accelerated planned moves to digital platforms. Remote access to information became a key requirement and platforms for online collaboration became instant must-haves. The continued shift towards cyber dependency has resulted in an increase in cybercrime.

World Economic Forum published a paper in January 2022 estimating the average cost of a cyber attack to be US\$ 3.6 million per incident. These costs are incurred over an average of 280 days and span the recovery of data and redesign of digital platforms. Below we explore the costs in more detail.





INITIAL RESPONSE TO A CYBERATTACK

Cyberattacks are carried out for ransom usually requested in cryptocurrency or to obtain data that can be exploited for gain or sold at a significant premium. In all cases, systems were breached and need to be secured, reconstructed and restored.

Once a cyberattack is identified, the first response is to shut down systems. This halts operations as all central platforms for transactions; operations and communication are not available. The cost of shutting down systems is difficult to measure as it encompasses the physical shut-down costs, the opportunity cost of halted transactions with customer, suppliers, employees and other stakeholders. Some companies continue operations by doing business outside the system. The costs of implementing manual controls to ensure that assets are not misappropriated during this time can be significant. Access and monitoring controls are especially important and management teams are required to be extra vigilant.

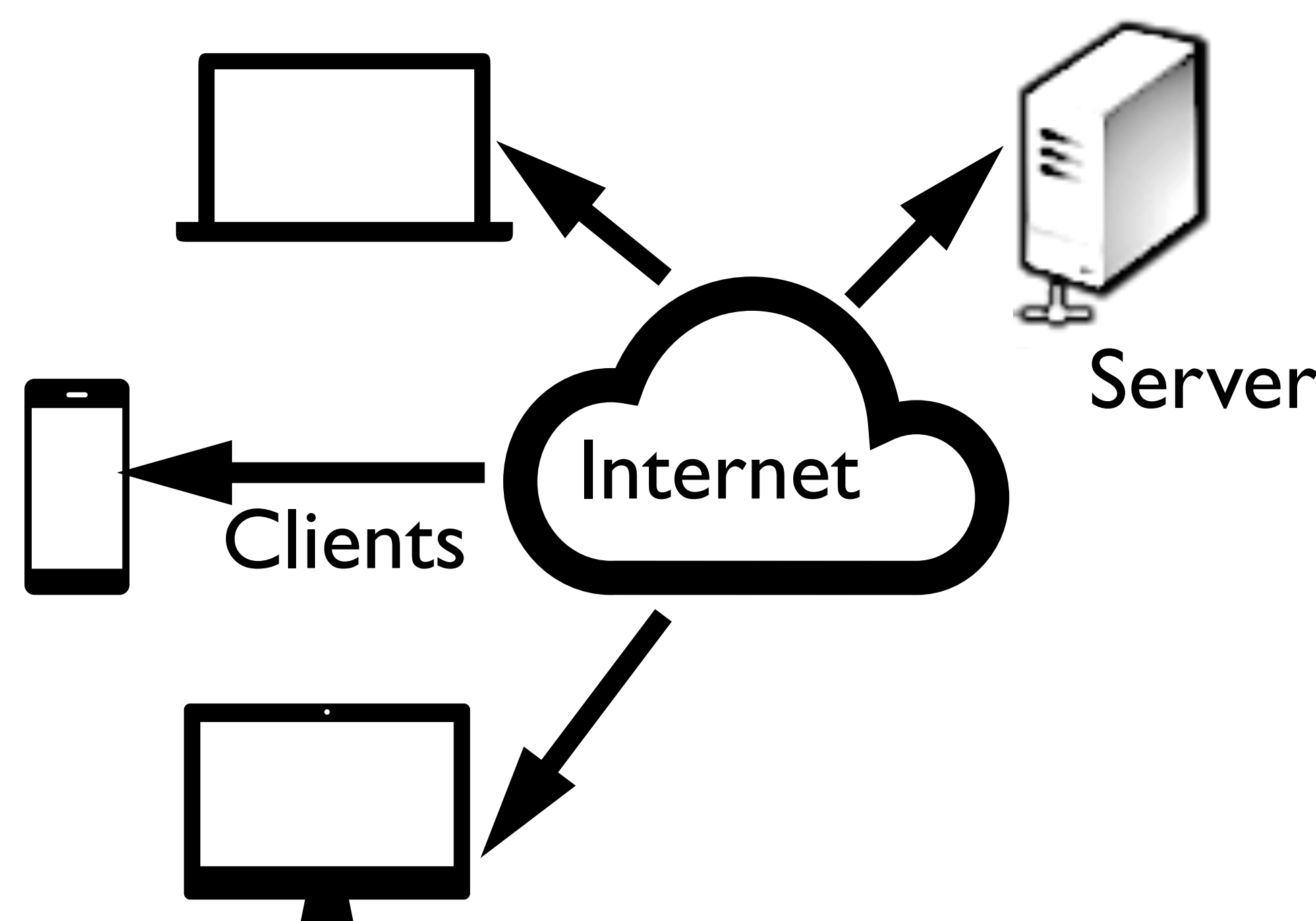
Companies additionally contract cyber experts to determine the nature, timing and extent of the cyberattack. System vulnerabilities need to be identified so that these can be secured prior to the company resuming online operations.

RECOVERY

Recovery of systems and data is usually phased and involves multiple layers of security be rebuilt before systems are

switched on. The first priority is to restore communication via email and telephone services. Each user is required to be tested and secured before being reconnected. For large companies with many employees, this can take a few days. To speed up the process, companies engage consultants to assist.

Data and systems that are maintained on the cloud can be recovered and restored quicker. Data stored on company or third party servers are assessed to determine the extent of the breach and takes longer to recover. Servers are first secured to reduce the risk of another cyber-attack, followed by the process of restoring the latest backups and testing backups for completeness against reported data or source documents. Depending on accuracy, timeliness and completeness of backups, this process can take between a few days and several months. The longer information takes to be recovered, tested and restored, the greater the contribution to business interruption costs.



Once the users and servers have been secured, networks connecting users to servers need to be secured to prevent another cyberattack. Companies try to reconnect users to servers as quickly as possible to cut business interruption costs. Often historical data recovery continues in the background while businesses resume normal transactions online. Network security forms part of the IT architecture and IT design review.

IMPROVING IT INFRASTRUCTURE & IT ARCHITECTURE

Many companies do not have complete inventories of IT Infrastructure nor documented IT architecture, and trying to determine all of this in the wake of a cyber-attack is difficult. IT infrastructure describes the components that make up a system, while IT architecture describes

the design of the components and their relationships. In fast growing businesses, IT architecture is forsaken in favour of business demands. A cyberattack alerts companies to the necessity of complete and accurate documentation of IT infrastructure and detailed planning of IT architecture even in environments where companies grow very rapidly.

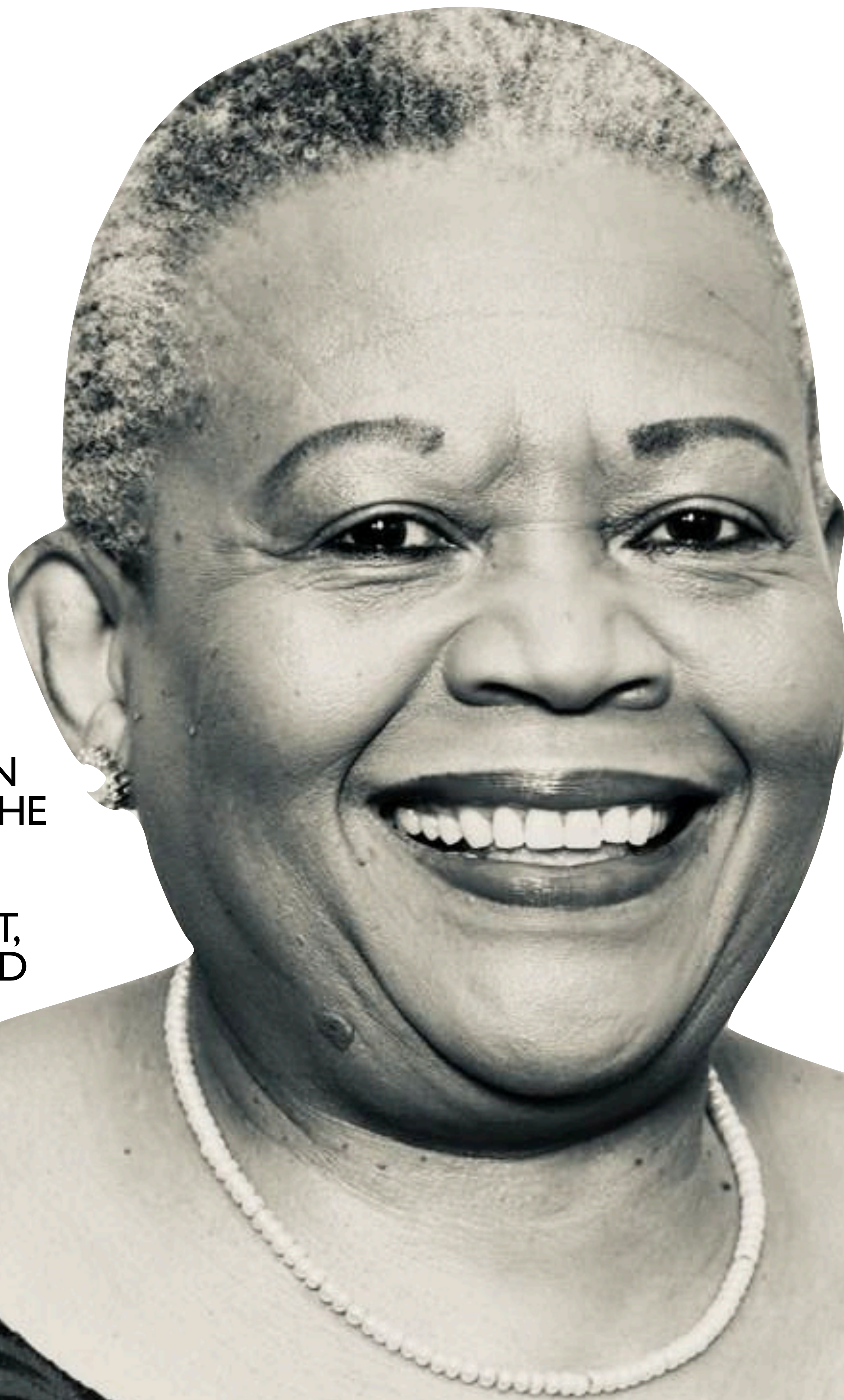
The economic turmoil caused by the coronavirus pandemic saw companies halting major investment spending and conserving cash resources. While digitisation was considered a necessary cost to do business during lockdown, the investment in IT architecture planning and cyber security was deemed a discretionary spend. Vulnerable digital platforms were ripe pickings for increasingly sophisticated cybercriminals. For antiquated or unplanned IT architecture, a cyberattack presents the opportunity to improve the design of IT systems but at a much higher cost as it is done under duress.

OUTLOOK

The continued increase in dependency of digital platforms necessitates cyber security be prioritised. With 39% of companies experiencing some sort of cyber incident in the last 2 years^[1], this is something that needs to be on every company's risk agenda. Collaboration between Chief IT Officers and Chief Financial Officers is essential to secure and prepare the company for the possibility of a cyberattack. Adequate investment in security and business interruption preparation not only reduces the risk of a cyberattack but also equips companies to better respond to a cyberattack.

Faatima Kholvadia is a seasoned finance professional with over 15 years experience in various industries, such as oil and gas, mining, chemicals, education and finance. Her skills range from Cyberattack Management, International Financial Reporting Standards (IFRS), Business Analysis and Process Improvement. Faatima is a qualified chartered accountant.

[1] World Economic Forum Global Cybersecurity Outlook 2022 – Insight Report – January 2022



ADVOCATE
PANSY TLAKULA,
CHAIRPERSON OF
THE INFORMATION
REGULATOR, ON THE
PROTECTION OF
PERSONAL
INFORMATION ACT,
HACKATHONS AND
THE METAVERSE

ADVOCATE PANSY TLAKULA

Chairperson of the Information Regulator

 SOUTH AFRICA

1. What were some of the unexpected challenges in your line of work?

Dealing with rapid digital transformation and change. There is a balancing act that is required. You are required to keep up with the pace of digitisation and technological change while ensuring that the entire team also keeps up despite differences in backgrounds and skills.

Leading and expecting outputs of a particular standard in a new environment where everyone is still learning.

2. How did you overcome them?

The emphasis has always been and is still on learning with the entire organisation, balancing mentorship with leadership. Leading by example and modelling the work ethic that I want to see from others.

Building shared vision – the capacity to hold a shared picture of the future we seek to create.

Having a great reservoir of patience because we don't learn at the same time, some take longer than others and if we have a shared vision, we need to ensure that we do not leave anyone behind.

3. Encrypted messages being hacked, what would the legal recourse be?

The Cybercrimes Act defines how any cybercrimes should be dealt with. Its main purpose is to reduce and prevent cybercrime in South Africa. It also helps law enforcement to enforce the law and hopefully protect the people of South Africa from criminals.

The Act creates cybercrime offences and prescribes penalties related to cybercrime. It provides overarching legal authority on how to deal with cybercrimes, by regulating how these offences must be investigated which includes searching and gaining access to, or seizing items in relation to cybercrimes

Offences include obtaining unauthorised access to, interception of or interference with data; computer-related extortion, fraud, and forgery; and attempt, and aiding and abetting regarding the offence.

The Protection of Personal Information Act (POPIA) also gives clear guidance on how security breaches can be dealt with and what legal recourse to follow as an individual or an entity.

“With technologies such as metaverse, it is important for South Africans to first understand the technology fully, its implications, weaknesses, risks that may result in cybercrimes and any challenges that the technology brings forth.

4. Are there any legal implications for entities when citizens experience data vulnerability when accessing sites on an unsecure connection (public Wi-Fi)?

The Independent Communication Authority of South Africa (ICASA) is responsible for regulating the Communications industry in South Africa. A licence is required whenever communications is carried from one point to another. Also, if entities want to deploy and operate a physical network, whether the network infrastructure consists of radio equipment for running a wireless network, fibre optic cables, copper-based lines, or switches, you are required to obtain a licence through ICASA.

The Authority also has extremely strict regulations and obligations to the service providers that provide these services. (ICASA Code of Conduct Regulations 2008), this outlines how operators are to protect and ensure the safety use of their networks.

ICASA's Consumer Protection unit was established to ensure the continued protection of consumers the broadcasting, telecommunications sectors. This is achieved through public-awareness programmes and a streamlined complaints-handling system.

ICASA has established a Complaints and Compliance Committee (CCC) is an independent committee of ICASA, established in terms of section 17A of the Independent Communications Authority of South Africa Act No. 13 of 2000 that specifically deals with complaints including breach of data. The CCC may recommend that one or more of the following orders be issued by the Authority namely:

- Desist order
- A fine/penalty
- Remedial action
- Amend or revoke licences; and
- Direct the licensee to comply with any settlement agreement, if applicable

Furthermore, the Electronic Communications Act, No. 36 of 2005 (the "ECA"), is the principal law regulating electronic communications. Amongst other matters, this law deals with the role of the regulator, the licensing of electronic communications services and systems, broadcasting services, the obligations of authorised service providers, the protection of users and subscribers, the power to make regulations and penalties incurred for breaches of the relevant legislation.

The South African Cybercrimes Act outlines in Section 3 - Unlawful interception of data that:

- Any person who unlawfully and intentionally intercepts data, including electromagnetic emissions from a computer system carrying such data, within or which is transmitted to or from a computer system, is guilty of an offence.

- Any person who unlawfully and intentionally possesses data, with the knowledge that such data was intercepted unlawfully as

contemplated in subsection (1), is guilty of an offence.

- Any person who is found in possession of data, regarding which there is a reasonable suspicion that such data was intercepted unlawfully as contemplated in subsection (1) and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

5. How does SA fair against the rest of the world in terms of Cyber protection given the fact that SA is moving swiftly into the digital space due to the covid 19 pandemic?

South Africa has implemented the following and it is on par with most countries in the world with regards to frameworks, acts and policies:

- Cybercrimes Act
- Cyber Security Hub which is a South African National Cybersecurity Awareness Portal consisting of Cyber Security Awareness Resources, CyberSecurity Campaigns, Cyber tips and Advice
- Protection of Personal Information Act (POPIA)
- South Africa's National Cybersecurity Policy Framework - The NCPF is intended to provide a holistic approach pertaining to the promotion of Cybersecurity measures by all role players

6. India's prime minister hosted a hackathon soon after coming into power to find the best hacker to train and use in government projects (streamline systems, e.g., home affairs, licensing etc). Would SA have the same capacity to host and train people in cybersecurity and AI?

Yes, South African is more than capable in training people in CyberSecurity and AI:

The South African Government through the Presidency has established the Commission on 4IR to formulate a strategy on how South Africa can position itself through policy review and programs to take advantage of the 4IR.

The Commission has developed the strategy which will inform the implementation of 4IR in South Africa. This has required partnerships between academic institutions, private business and government to work together in ensuring that the right skills that meet the technology innovation requirements are available. The SA government collaborates with academic institutions, for example in South Africa the Centre for Artificial Intelligence Research (CAIR). Additionally, the Department of Communications and Digital Services has established a CyberSecurity Hub Project

The Cybersecurity Hub* is the national Computer Security Incident Response Team (CSIRT). Its objective is to create a

Cyberspace an environment where all residents of South Africa can safely communicate, socialise, and transact in confidence. The Cybersecurity Hub collaborates with stakeholders from government, the private sector, civil society, and the public with a view to identifying and countering cybersecurity threats. In creating the secure Cyberspace, the Cybersecurity Hub initiated Cybersecurity Awareness and part of the cybersecurity awareness initiatives was the development of the national cybersecurity awareness. The Awareness Portal is the repository for all

Cybersecurity Awareness information and is used for the dissemination of Cybersecurity Awareness programs and information. Other Cybersecurity Awareness initiatives include the following:

1. *Community Radio*: Deputy Minister hosts one-hour program at GCIS studios - broadcast on approximately sixty-five community radio stations, to approximately five million people. The first program focused on financial security, with SABRIC as a participant discussing financial security topics.

2. *Cyber Schools Toolkit*: A Cyber Safety and Awareness Toolkit for school learners was developed, in partnership with UNISA, UK government and its objectives is to promote a cybersecurity mind-set and culture through an educational toolkit.

3. *"Qaphela Online" Newsletter*: The newsletter is aimed at encouraging South African citizens to be vigilant when surfing the Internet. Various Stakeholders work with the Cybersecurity Hub in developing monthly newsletter focusing on different themes.

4. *Hackathon*: The Cybersecurity Hub has been collaborating with a consortium of private sector organisations – including KnowBe4, TrendMicro, BCX, Bi-Technologies, Vox Telecom, NClose, Black Rhino and Bi-Tech Africa - and the University of the Western Cape's Future-Innovation Lab and hosted a cybersecurity themed hackathon, called the Government Innovation Challenge.

7. Facebook recently released information regarding Metaverse meeting rooms, where your avatar could brainstorm business ideas online. What would the legal recourse be against

intellectual property and business innovation, should the meeting room be hacked? What precautions should organisations take?

The Metaverse is a digital space where people can connect and interact with each other. It is an exciting idea, and it will be interesting to see how it develops in the future. For businesses, this provides opportunities to reach out to new markets and customers. The idea of Metaverse South Africa gives businesses the opportunity to connect with their target market and should be explored further.

With technologies such as Metaverse, it is important for South Africans to first understand the technology fully, its implications, weaknesses, risks that may result in cybercrimes and any challenges that the technology brings forth. In understanding the technology, you can fully prepare or at least prevent any risks

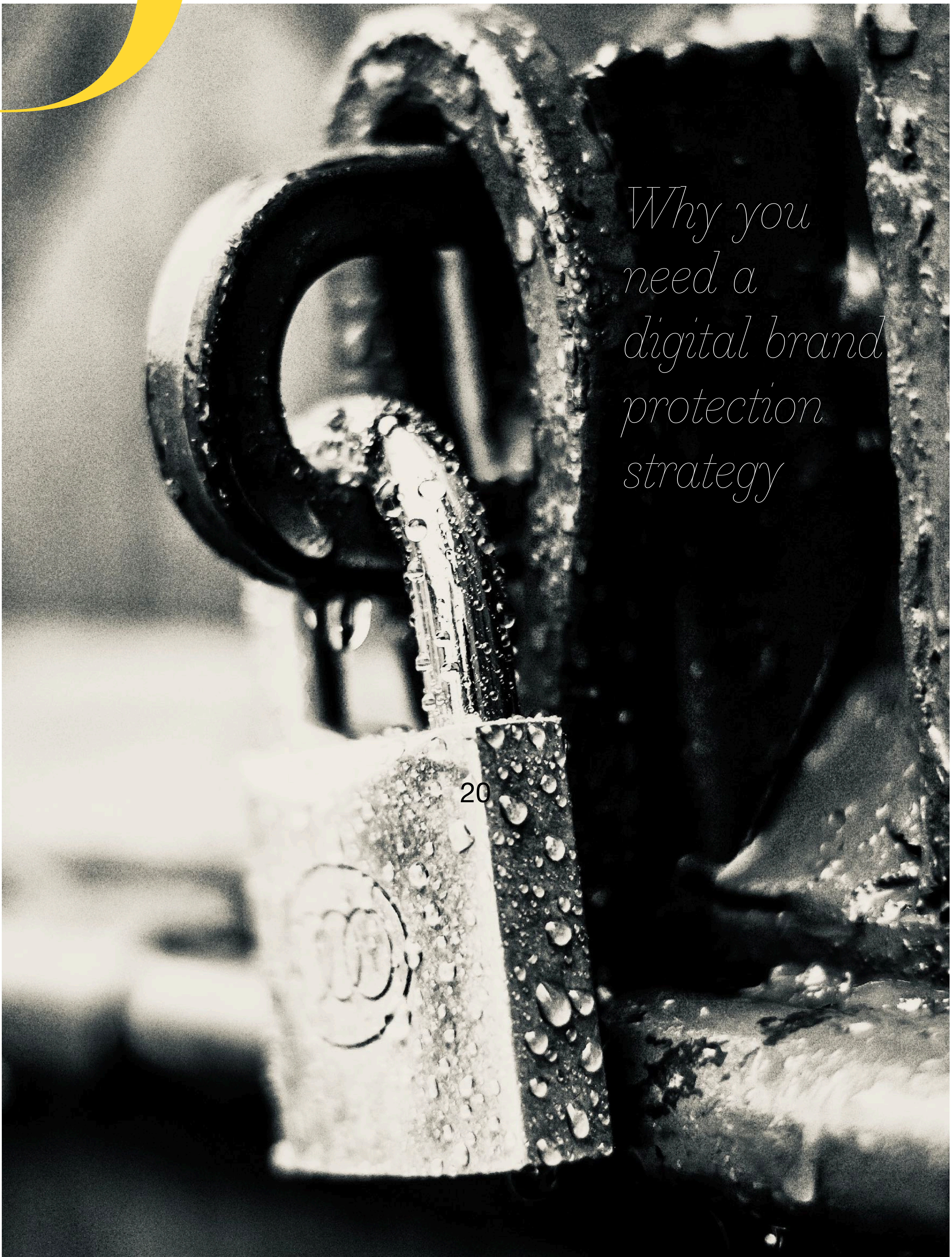
With that said, our organisation would implement very strict Security Policies, Security Controls, Privacy Policies, and other Regulations before introducing this technology

When Covid 19 started, the country was not fully prepared as some of online meetings were not controlled and you will see uninvited guests participating in these meetings.

Our organisation has learned from all these mistakes and will ensure that Metaverse is fully understood and that appropriate controls such as access control, authentication, identity management, awareness and the traditional cybersecurity controls should be fully implemented.

* More info : <https://www.cybersecurityhub.gov.za/cyberawareness/index.php/awareness-resources.html>

Digital Brand Protection



*Why you
need a
digital brand
protection
strategy*

20

Receiving dubious emails from bad actors requesting you to access your bank statement or tax profile is a common occurrence. These bad actors utilise your digital brand assets to carry out these scams. They understand that your company's brand helps distinguish your

organisation on the business landscape and from your competition making your brand prey to their schemes.

“The benefits far outweigh the costs of initialising or putting into effect your strategy. Your organisation’s reputation is protected.

Bad actors are increasingly using your online brand as bait, launching copycat websites to trick customers, partners and stakeholders into divulging credentials, sensitive information and even paying them. These attacks often put your brand and reputation at risk. Brand reputation damage has negative repercussions, it dilutes the strength of the brand and in the end, has negative financial impacts.

It is not just fakes that we should be concerned about. There’s a whole world of other issues to consider; from phishing scams, website lookalikes, counterfeiting, content copy, cybersquatting, typo-squatting, false claims of affiliation, reputation attacks to social media impersonators, to regulatory breaches that could create headlines for all the wrong reasons.

PROMINENT TYPES OF BRAND INFRINGEMENT

Counterfeiting: The creation of an identical product to an existing product of your company made by a third party to deceive customers into thinking the counterfeit is an official item.

Copyright Infringement: The unauthorised copying, display, distribution, or performance of any of your company’s works that is copyright protected.

Trademark Infringement:

Trademarks are your mark of origin used to differentiate your company’s products or services from others.

Patent Infringement: The act of making or selling your company’s patented products without our permission.

Design Infringement: The manufacture of goods using patented design features to create a similar unauthorised version of our product.

You need a brand protection strategy that will not only protect you from the above infringement scams beyond your email perimeters but to proactively uncover and takedown attacks in their early stages. The strategy should aim to evolve from a perimeter-based strategy to a more proactive pervasive one that will protect you and in the event of an attack ensure resilience.

The benefits far outweigh the costs of initialising or putting into effect your strategy. Your organisation’s reputation is protected. Your customers and supply chain are protected from fraud and kept safe from harm against online attacks using your brand’s digital assets. Attacks are mitigated before they become active as instant action is taken to block suspicious and malicious domains and URLs. Revenue increases as a managed service will reduce the cost and labour overhead on IT, security teams and legal. Boost legal efficiency and your organisation remains compliant with governing laws

An effective brand protection strategy must align with your overall strategy and should focus on domain

monitoring and monitoring your brand in Key Market Places. You need to focus on developing a social media brand voice that connects you with your audience. One that will aid your stakeholders to discern when your brand has been compromised in the event of phishing scams or copycat websites. These focus areas require the initiation of plans that successfully mitigate potential threats to your organisation’s brand. To achieve this, an aligned effort will be required by both the business and your marketing department.

A fully managed service approach is required that discovers threats by gathering intelligence on infringement. Prioritises the largest threats and highest risks to your brand and consumers. It should take action against prioritised threats strategically and at scale with a lasting impact.

The managed service’s technology will utilise tools that monitor and identify brand abuse and IP infringement. Technology tools that will scour and scan the internet for infringements, allowing identification of the most prolific and financial injuring infringers by prioritising them. As well as enabling you to act swiftly and with impact. Ensuring that you don’t suffer further loss of revenue, reputation, or consumer trust.

The internet has made it easy for criminals to target organisations, but it also holds the key to the problem too. By leveraging Brand Protection technology solutions, collective expertise, and shared insights, we can – work together. Internal and external collaboration is key. Collaboration will ensure that your consumers are protected, and you receive maximum return on investment from your Digital Brand Protection Strategy.

Cybercrimes Act



The advent of the Covid-19 pandemic has brought a new reliance on electronic devices, and, therefore, crimes related to cyber security vulnerability and breaches such as internet fraud, email hacks and having one's privacy comprised by hackers and other entities have become commonplace. The spike in cybercrimes has made governments consider adapting existing cyberlaws to deal with the on-going metamorphosis to the 4IR.

1. What is the current impact of cybercrime in SA?

South Africa has one of the highest numbers of cybercrime victims worldwide, and costs the country billions a year. Everyone in South Africa has been a victim of cybercrime, whether it was successful or only an attempt.

2. Why is the Cybercrimes Act 19 of 2021 needed?

It is needed to provide a framework for how different cybercrime offences will be dealt with and the sentencing of those offences. Previously South Africa had the Electronic Communications and Transactions Act 25 of 2002 (ECT Act) which had a legal framework for offences. The new act repeals the relevant provisions in the ECT act. If someone is found to have committed an offence in relation to the act they can be prosecuted with a maximum penalty of a fine or imprisonment.

3. Certain parts of the Act have commenced and others haven't due to lack of enforcing agencies amongst other reasons. What would you say is the reason for this?

The following sections will not yet commence namely:

Part VI of Chapter 2 which deals with issuing of Protection Orders which can be granted against a suspect of Cyber Harassment, Cyber threats of damages to property or anyone inciting other to damage property and Revenge Porn. Section 20(1) of the Cybercrimes Act provides that a complainant who lays a charge with the South African Police Service (SAPS) that an offence contemplated in s 14, 15 or 16 has allegedly been committed against them, may, on an ex parte basis, apply to a magistrate's court for a protection order, pending the finalisation of the criminal proceedings.

Section 38 (1) (d)-(f) which provides for any person who unlawfully or intentionally gives false information under oath or by way of affirmation knowing it to be false or not knowing it to be true, with the result that an expedited preservation of data direction contemplated in Section 41 is issued or a preservation of evidence direction contemplated in section 42 is issued; or a disclosure of data direction

contemplated in section 44 is issued, is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and imprisonment. Section 40 (3) provides that an electronic communications service provider is required [1] to provide an electronic communications service which has the capability to store communication-related information and not required to store communication-related information in terms of a directive issued in terms of section 30(2) of that Cybercrimes Act must, in addition to any other obligation imposed by any law, comply with a real-time communication-related direction in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available.

The Non-Commencement also applies to the Direction for expedited preservation of data as contemplated in section 41 of the Cybercrimes Act, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer, Section 42 of the Cybercrime Act which deal with preservation of evidence direction in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer will not apply.

The non-commencement will apply to a disclosure of data direction contemplated in section 44 of the Cybercrimes Act, in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer that was preserved or otherwise stored by the electronic communications service provide or any order of the designated judge in terms of section 48(6) of the Cybercrimes Act in terms of which the electronic communications service provider is ordered to obtain and preserve any real-time communication-related information; or obtain and furnish traffic data.

4. What are the substantive Cybercrime provisions in the Cybercrimes Act?

Various sections in The Cybercrimes act provide for unlawful and intentional access; unlawful interception; unlawful acts in respect of software/hardware tools; interference with data; interference with data or computer programs; unlawful interference with storage mediums; unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data/device(s); aggravated offences in terms of the Act; theft of incorporeal property; malicious communications including incitement to violence or causing damage to property; revenge pornography; and attempting, conspiring, aiding, abetting, inducing, inciting, instigating, and instructing or procuring another to commit a criminal offence. The discussion of the provisions of the Cybercrimes Act ends with a consideration of sentencing for offenders found guilty of having committed cybercrimes, as well as of court orders to protect complainants during the course of criminal proceedings.

Section 2 of the Act makes provision for an offence in relation to the unlawful securing of access in respect of a computer system or a computer storage medium. This section provides that any person who unlawfully and intentionally secures access to data, a computer program, a computer data storage medium or a computer system is guilty of an offence.

5. Does the new act deter criminals from committing cybercrime?

The act has strengthened the substantive (the dos and don'ts) and procedural law (the how to get the evidence and prosecution of cybercrimes) relating to cybercrimes. The penalties in section 19 are more stringent as in the earlier ECT Act which only had penalties up to 5yrs and a fine. Section 19 currently prescribes penalties currently between 5-15yrs and a fine. Effectively being a deterrent to people who commit cybercrimes.

[1] In terms of section 30(1)(b) of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002,

6. What is the impact of the Cybercrimes Act considering SA loses R2.2 billion annually to cybercrime?

The Act has been in effect for 10 months and as much as it is early days, sections 14 & 15 have been used to prosecute offenders using electronic communication devices to threaten person, intimidate persons & or threaten their property.

Section 8,9,10 extensively deals with cyber forgery and uttering, ransomware attacks, in the form of cyber extortion as well as 419 schemes in terms of the cyber fraud provision.

Section 12 prescribes that the theft of incorporeal property as included in the common-law offence of theft is now codified and includes electronic theft of an incorporeal

7. What are the most common forms of cybercrime people should guard against?

Spoofing, spamming, ransomware and phishing. 8. Are companies doing enough to protect themselves from cyberattacks? Yes and No. Yes companies are aware of cybersecurity vulnerabilities. In terms of section 19 of the South African Protection of Personal Information Act Act they have a positive duty to keep personal information safe and secure. Additionally in the event of a cyber breach there is now a duty to report all data breaches in terms of section 22 of POPIA Act.

9. Whom should corporates report an attack to?

Report to the affected data subject, local authorities, and

information regulator. They also need to report to their international data subjects' authorities and regulators.

10. How much time do they have to report the attack?

Within a reasonable time. Although a reasonable time is not defined one can look at the GDPR which stipulates 72 hrs. Section 22 states that one has to consider the legitimate needs of law enforcement in investigating a cybercriminal attack and the restoration of the affected system.

11. What are the consequences of corporates not reporting cyberattacks?

Section 54 of the Cybercrime Act states that an electronic communications service provider must, within seventy-two hours of having become aware, report an offence committed in terms of Part I of the Act

12. Does the act protect South African organisations that are attacked by foreign bad actors,

are there any limitations concerning foreign attackers?

The act gives law enforcement agencies the power to be aggressive and skilful in pursuing cybercriminals locally and internationally. It gives local authorities extensive powers to work with international law enforcement agencies to investigate, search, access and seize items that will aid their case.



Prof. Sizwe Snail KA Mtuze is the Senior Partner at Snail Attorneys @ Law and has been appointed Adjunct Professor in the Mercantile Law Department of Nelson Mandela University (NMU) Law Faculty. He is also co-editor and author of Cyberlaw @ SA 4.

LANRE OGUNGBE

The Rising Threat of CyberAttacks on *AFRICAN FINTECHS:* *the way forward*

📍 NIGERIA

LANRE OGUNGBE IS THE CO-FOUNDER AND CEO OF IDENTITYPASS. HE DELVES INTO CYBERATTACK THREATS FACING FINTECH AND OFFERS STRATEGIES TO MITIGATE CYBERATTACKS.



The outbreak of COVID-19 and the ongoing situation between Ukraine and Russia proves how the cyberworlds are going beyond borders. Recently, the threat to cybersecurity in the African financial service sector has experienced a significant increase. This is partly attributed to the high usage of sophisticated technologies, an insufficient supply of cyber talent, and companies worldwide supporting largely remote workforces. Fintechs are constantly battling the challenge of securing their platforms and customers from cyber thefts, while people remain skeptical of sharing their data online.

Africa recorded a massive increase in fintech startups in 2021, with over 576 fintech companies sprouting up. Nigeria houses over 200 of these fintech companies,

South Africa, has about 154 fintech startups, and Kenya has over 93 fintech companies. Together, the three countries foster over 65 percent of African fintech attracting over 2.1 billion U.S. dollars in venture capital (Statista, 2021)

However, today, financial losses arising from cyber threats are escalating. In 2021, cybercrime reduced Africa's GDP by 10%, resulting in a \$4 billion loss. As internet usage continues to increase, expanding 5G networks connected devices at faster speeds and greater bandwidths, so does the amount of personal information and data made available online. According to Kenya – based IT advisory firm Serianu, cybercrimes cost African economies \$3.5 billion in 2017.



In the Middle East and Africa, 94% of companies admitted they had suffered a cyber-attack in 2021. 48% of these attacks resulted in damage of over \$500,000. The South African Banking Risk Information Center (SABRIC) reports that South Africa loses \$157 million annually to cyberattacks.

Though the number may even be higher: not all companies detect (or admit) they had breaches as hackers are getting much better at disguising their attacks, so they can remain undetected and extract more data. Furthermore, with more customers and corporations embracing digital transformation, more data are available in digital formats producing new security challenges for fintech.

In the African landscape: the threats in fintech sectors include ransomware attacks, Business Email Compromise (BEC) attacks, CEO fraud, account compromise and hijack impersonation, and data theft. Social engineering has metamorphosed into crafting more sophisticated phishing links and harvesting PII data of corporate staff on social media platforms. Also, there are more cryptocurrency heists: wallet phishing and fake wallets. The increasing adoption of cloud infrastructures also comes with the threat of data leakage due to the misconfiguration of services.

Some of the top Fintech cyber threats experienced in Africa within Q1 2022 are highlighted below:

Phishing

Phishing is a cybercrime that targets(s) via email, phone, or SMS by someone or a fake company posing as a legitimate entity to trick people into giving out sensitive information. These include personal identification information, banking, and disclosing credit card information and passwords. In 2020 alone, Sophos reports that 66 percent of IT teams in Nigeria revealed that the number of phishing emails targeted at their employees increased. This stems from the fact that

Malware & Ransomware

An average of 1,848 ransomware attacks per week target an organisation in Africa compared to 1,164 globally. Among the significant malware samples in the African terrain are trojans, Info stealers, Agent Tesla, Lokibot, and Dorkbot. HilalRAT has been observed to target the financial industry in Ghana, Kenya, Mozambique, Nigeria, South Africa, Tanzania, Uganda, and Zambia. Victims of Kaseya ransomware spread to Kenya and Uganda in East Africa. Most Businesses within the payment space susceptible to these attacks are those yet to implement the required resources to tackle them.

Leakage of Sensitive Data

All application data, including preferences and files, is stored in a single directory per application. Generally, only one application has direct access to this directory, and no other application can access it. But because both operating systems allow data from an application to be shared, when a leak happens, scammers take hold of the opportunity to perpetuate severe attacks that will eventually negatively affect businesses.

Account Hijack, Identity Theft, and Defacement

Brand identity and credential theft in the form of hijacking official social media accounts to impersonate organisations are increasing in Africa. There have been cases where actors clone popular fintech Twitter handles to defraud unsuspecting clients with a claim of providing support on banking issues. Users willingly disclose confidential information like BVN, login credentials, etc., in the process. Most techniques are perpetuated by sending fake links to download pirated applications, free proxies, and VPNs. Another popular approach includes impersonating customer support on Twitter and demanding credentials and personal

Identity of customers in an alleged troubleshooting session.

The yahoo boys of Nigeria and Sakawa boys of Ghana are the prominent players in this fraud industry. However, credential mining and wallet phishing are also very observable in major parts of South Africa. Common tactics include mobile sim card swapping and cloning, which is more prevalent in Kenya. These actors also use digital extortion: sextortion and blackmail schemes.

PROVEN STRATEGIES FOR MITIGATING AGAINST CYBERATTACKS

To address the cybersecurity challenge for fintech, African fintech companies are strengthening their cybersecurity defences with new and improved ID solutions. Here are some preventive strategies that are effective against various cyber attacks.

1. Mitigations for Phishing attacks

It is of utmost importance that African companies use two or more means to authenticate their system. They should ensure security awareness training: phishing simulation and social engineering awareness program combined with an AI-driven KYC solution.

2. Mitigations for Malware attacks

African Fintechs must implement disaster recovery plans; regularly test data backups for restoration of organisational data; enable versioning in cloud environments to maintain backup copies of storage objects, among others.

3. Mitigations for Data Leakage

Ensuring information is encrypted and stored to PCI DSS compliant standards, use of data loss protection. Ensuring all sensitive data, such as customer PINs and passwords, are stored in encrypted format throughout the systems and databases. Furthermore, fintech operators in Africa should protect

data from external access by using multiple levels of firewalls.

4. Prioritizing Security-by-Design

Not incorporating security by design is costly and puts a business in a vulnerable position. Though the African financial technology sector has come a long way, there is still a need to include cyber security from the onset. The primary security control and best practices include:


- Effective backup and recovery to prevent data loss.
- Avoid using untrusted and outdated website components: plugins, libraries, proxies, and pirated software.
- Implementation of multi-factor authentication for the administrator, and sensitive accounts, other backend login directories
- Utilize a safe API and positive server-side input validation.
- Use security controls like Web Application Firewalls for Websites and endpoint detection and Response for endpoints resources.
- Adopting effective Cyber insurance in case of a breach
- Integrate threat intelligence into security solutions and control to stay up-to-date with attackers' behaviours.
- Ensure regular software updates to mitigate exploitation risk, carrying out vulnerability and continuous assessment exercises.

As most African financial services companies embrace digitisation and new methods of supporting customer interactions, the attack "surface" expands. Professional hackers are constantly adopting new techniques. It is, therefore, critical that, now more than ever, African financial services firms develop robust security blueprints to improve risk management.

Contact Identitypass for your AI-powered and robust KYC and compliance needs.

BLACK SEAL

SIM PROTECTION

A person wearing a dark hoodie is holding a smartphone. The background is dark with numerous white numbers floating around, creating a digital or data-like atmosphere. There are also two white padlock icons, one on the left and one on the right, suggesting security or hacking themes.

**THE FIGHT AGAINST
PHONE
HACKING
BEGINS HERE**

HOW YOU GET HACKED

Traditional phone service providers get thousands of requests for new SIM cards every day, most of which are legit. Because their processes are geared towards efficiency, they don't do detailed checks to ensure that the person requesting that SIM card is actually you.

WWW.BLACK SEAL.COM

WHAT IS A SWIM SWAP ATTACK?

A SIM swap is a type of social engineering attack, in which the hacker fools or bribes a phone service provider into porting the victim's phone number to the hacker's device. Once they have your phone number, they can use it to gain access to other accounts, including bitcoin wallets and other financial accounts. This is huge, because phone numbers have become the way we access almost every other service.

INSURANCE COVERAGE

The logo for Lloyd's, featuring the word "LLOYD'S" in a white, serif font on a black rectangular background.

Black Seal Protection has a 100% success rate to date: not a single client has been SIM-swapped on our secure cellphone plan. We intend to keep it that way.

No security system is complete without a failsafe, however. In the unlikely event of a hacker taking over your phone while on our plan, we provide cybersecurity insurance worth \$5 million through Lloyd's of London. This means you're covered if money is stolen from your online accounts as a result of a SIM swap attack.

WHAT YOU GET

Black Seal Protection works like any other carrier, except Black Seal adds exceptional security to your plan via an impressive security tech stack.

Black Seal replaces your current phone plan with coverage from one of South Africa's two top mobile networks. We'll send you an encrypted SIM card to put into your existing phone. You can keep using your existing phone number, or we can give you a new one if needed.



Unlimited call, text, and data.



International data roaming*
(*eSIM compatible).



5G network speed,
availability, and ultra-low
latency



Passionate 24/7/365 customer
service

CONTACT US :

info@blacksealprotection.com
+27 82 365 6715



EFFECTIVE COMMUNICATION

in the event of a cyberattack

Organisations require effective crisis communication strategies as in this current age it is not about if a crisis will occur, but when. This tells you that you need to be prepared for when it happens. You want to foster relations through communication with your stakeholders that breed trust and respect. The following will aid your organisation's resilience in the event of a data breach.

Mechanisms required to best prepare for an attack

The defining factor in how well your company and its reputation weather the data breach storm is crisis preparedness. Have an effective crisis communication plan that encompasses a cyberattack strategy. The plan should have guiding principles, approval structures, outline potential scenarios, and templates for internal and external statements. The plan should prioritise post-event goals that:

- protect the data subject
- manage key stakeholders

- protect sales and ability to operate and trade
- stock market value
- minimize the company's reputation damage
- minimising the cost of the breach to the business

The company's cell phone policy should include the employer's right to have employees' cellphone numbers to communicate critical information. The policy should be part of onboarding and reside on the intranet.

Who should communicate the breach?

Leadership is most tested during a crisis and effective management and leadership will help navigate an organisation through a crisis. Ensure the Chair/Managing Director/CEO delivers the message. Frame the message by accepting responsibility for the breach and apologise. The leader should take care to prioritise and address each stakeholder's concerns and queries, this will aid in the organisation emerging stronger and more resilient. Leaders who want an engaged workforce during the cyberattack will empower their



managers to support their departments and manage their external stakeholders.

When to communicate the breach to stakeholders?

Not all breaches require immediate action, therefore access the situation according to the cyberattack communication strategy you have in place before you communicate. Should a ransomware attack take place, time is of the essence and an urgent and aggressive communications posture is required. Your employees will be waiting to hear from you to lessen the deafening radio silence that causes confusion, uncertainty and worse distrust among staff. Communicate quickly to employees. Prolonging communications will increase the impact of the crisis and it will also affect the multiple communication methods you have in place. Ensure that the communication is clear and actionable. Ensuring composure among staff is key. Achieve this by constantly updating employees with the most current information directly from the company head. Employees might receive misinformation from outside sources such as social media which will cause employees to lose trust in their leaders.

Additionally, a data breach that affects external stakeholders (customers, patients, suppliers, etc) in which their personal information and identification are stolen represents a serious breach of information and poses a substantial threat to the company, its partners and users. Notify your data subjects immediately and address their feelings of vulnerability. They need to hear it directly from you. Keep them in the loop with clear and easy-to-understand messaging with 4 important points:

1. A brief overview of the incident

2. What customers need to remain protected
3. The precautions you will have in place to mitigate future occurrences
4. How you are working with law enforcement authorities to bring perpetrators to justice

“Notify your data subjects immediately & address their feelings of vulnerability. They need to hear it directly from you.

The South African Protection of Personal Information Act (POPIA) and the European Union's General Data Protection Regulation (GDPR) require you to take appropriate action following a breach. Report to the authorities and the Information Regulator. The South African Cybercrimes Act Section 54 states that Electronic Communications Service Providers (ECSPs) and financial institutions have 72hrs to report cybercrimes to the police. Note the section has not come into effect as yet and will commence on a future date. Companies that operate past South African borders are liable to report security data breaches and incidents to the affected countries' local authorities and regulators. The GDPR has financial penalties for serious failures – up to 2% of annual global turnover or 10 million Euros, whichever is higher. Ensure that you are accustomed to the regulations of the regions you operate in.

How to communicate a breach to stakeholders

Employees are your biggest asset; they will have to be kept in the loop immediately when IT systems go down. During an attack VoIP-based phone systems may get lost, websites hosted internally may go down and if your network is compromised all computers become stand-alone machines.

This might be a challenge post covid as most organisations manage dispersed workforces. Your strategy should encompass multiple communication channels that reach all employees. Mass notification systems are required to alert staff of data breaches, security outages or any other emergency. The system should reach all employees, and factor in different work schedules and time zones for international organisations. Send out an email, phone calls, SMS, WhatsApp, desktop notifications and other channels such as conference bridges.

To communicate with data subjects use all available channels to increase reach. Use direct forms of communication such as tailored emails to target specific groups, your website with FAQs, toll-free numbers, personal calls, social media to clear rumours and negative perceptions and traditional media made up of trusted journalists to disseminate information.

Correctly tackling the above can make a substantial difference in how your stakeholders respond to the news. It will aid your company to emerge from a security breach and retain the loyalty of all stakeholders. A cyberattack is a difficult maze to manoeuvre, but if managed correctly through effective communication it's an opportunity to come out stronger.

DEBBIE BOTHA

IN ADDITION TO HER ROLES AS WOMEN IN AI'S GLOBAL CHIEF PARTNERSHIP OFFICER AND MANAGING DIRECTOR AT DALEBROOK MEDIA, MIDDLEEAST. DEBBIE IS A CERTIFIED IBM THOUGHT LEADER INFORMATION ARCHITECT, AND A DISTINGUISHED IT ARCHITECT.

DEBBIE IS ALSO THE RECIPIENT OF A LIFE TIME ACHIEVEMENT AWARD FOR HER ROLE IN TECH LEADERSHIP, HELD RECENTLY BY THE BERKELEYME INVESTORS CLUB WOMEN DIGITAL START-UP INVESTMENT CONFERENCE IN ABU DHABI.

HOW TO *KEEP* WOMEN IN TECHNOLOGY

📍 UNITED EMIRATES

When it comes to Diversity and Inclusion, my experience throughout my career in has always been amazing. When we talk about Diversity and Inclusion, we need to talk about it on Board and C-Suite level, the strategy tables on all levels of the organisation, the teams and the solutions. Our teams and managers, even the executives were always an equitable diverse set of people, from when I started as a Cobol and Natural Adabas programmer on the IBM Mainframe in the early '90s, through to leaving IBM South Africa as an Executive Information Architect in 2017 to work for IBM in UAE.

At IBM, I was fortunate to become involved in all kinds of Emerging Technology, specifically Artificial Intelligence initiatives. It is there where I really started to understand that it is not only the people in the organisation that has to be diverse, it is also the technology and data that crucially need the diverse perspectives.

“

AI IS THE ONE PROFESSION THAT CAN EITHER TREMENDOUSLY BENEFIT SOCIETY IF DIVERSITY AND INCLUSION IS DONE RIGHT, OR HURT SOCIETY IF DIVERSITY AND INCLUSION IS NOT BAKED INTO EVERYTHING THE ORGANISATION DOES.





We are living in this incredible inflection point in history due to unprecedented advancement in technology, the explosion of data and our ability to consume and convert it into intelligence. We are at the start of a seismic technological shift that occurs only once every 25 years and it will be driven by Emerging Technologies, especially artificial intelligence.

Today more than ever, diversity is important for organisations to be successful. We know that organisations with equitable female representation in the C-suite and boards report 10% better economic performance.

Organisations will be incumbent disruptors with the rich historical data that they have, especially about their consumers. These organisations clients create this Vision of how they will unlock the value of Data and AI in the future. Randy Bean and Thomas Davenport wrote books and many articles about practical strategies and examples of AI bringing great economic benefits to organisations. For example in healthcare the benefits in oncology is clear, but also administratively, AI help to greatly improve supply chains and scheduling of hospital staff. Doctor overtime can be reduced with

10% and facility utilization can be increased with around 15%.

AI is the one profession that can either tremendously benefit society if diversity and inclusion is done right, or hurt society if diversity and inclusion is not baked into everything the organisation does.

Last year a World Economic Forum article stated, “Bias in AI is a real concern and it’s generating more attention. Gartner predicts that in 2022, 85% of AI projects will deliver erroneous outcomes owing to bias in data, algorithms or the teams responsible for managing them.”

Large Health Insurers can save billions of dollars applying AI in Fraud, Wastage and Abuse in healthcare payments. In patient care, extensive validation and testing has to be done to ensure Responsible AI. Responsible AI means that your AI Algorithms are human-centric. Andrew Ng, the famous founder of Coursera, started the Data Centric AI movement to address amongst other things the bias that is prevalent in AI in all industries. We have many examples of AI solutions that are biased. The AI Thoughtbook lists over 200 cognitive biases. One example is patient treatment in healthcare, where you are treating a black person with a treatment that was only tested with data of white people. Another example could be a team of young males developing AI algorithms for recruitment, using data that is more skewed towards information they have about male candidates.

Why is it so biased? It is because today worldwide not more than 26% of the field of data, analytics and AI are women. We are not encouraging enough women to enter the field.

It is because only 10% of worldwide publications in this field are by women. Women are more likely to be taking up roles that are more supportive, and not driving innovation and change.

It is because worldwide 50% of women in the field leave in their mid-careers. Research has shown that many women see the corporate ladder as a difficult obstacle, while men see it as a welcome challenge. Most men thrive at convincing others that they are ready to be promoted, whilst most women prefer that their work speaks for itself. There is the phenomenon that women in their 50s are more likely to develop imposter syndrome, feeling that they don't belong, and especially because the higher up they go in the corporate ladder, the less females they encounter. Research also shows

that women list less skills on their profiles, and will only apply for a position when they are confident that they are experts in 85% of the skills or requirements listed. Men will apply for the same position when they feel that they know enough about 40% of the skills listed. Another set of research indicates that when looking at performance appraisal history of large corporates, women are consistently rated with less promotion potential than their male counterparts, even if their current performance is higher than their male counterparts,

How do we do it right? We encourage more women to enter the field. We encourage women to not only take on supportive roles but participate and lead. We encourage women to stay in the field, become Trailblazers and give back to the field.

According to World Economic Forum, and specifically two wonderful female leaders, Kay Firth Butterfield and Beena Ammanath, there are five ways to increase women working in AI – supporting STEM Education, showcasing female AI trailblazers, mentoring women for leadership roles and creating equal opportunities. Ensuring a gender-equal reward system is an absolute necessity as well. Global organisations are doing great work to help women play a key role in the AI sector, but these efforts need to be bolstered to make a tangible difference at scale.

It was mainly based on this advice that Women in AI (WAI) started identifying and recognizing women in AI Trailblazers, and Kay Firth Butterfield is one of them.

WAI is on a mission to close the gender gap in Data, Analytics and AI on all levels. Helping companies of all types, sizes and industries with Diversity and Inclusion and Responsible AI, from Boardroom to C-suite, to the strategy tables, teams

and solutions. It is important to ensure equitable diversity, not skewing towards more women than men, as then a whole other set of biases will creep in.

WAI is a non-profit do-tank working towards gender-inclusive AI that benefits global society. WAI is bringing all minds together across 150 Countries, making change happen with more than 10,000 members and changing the role of Women in AI with 200 volunteers. It is a vibrant community with more than 32,000 LinkedIn followers.

WAI and its strategic partners have developed great programs to provide a safe and engaging platform for women to grow in their career in AI, both technically and in terms of leadership and eminence, inside the organisation and outside the organisation. The beauty of this platform is that these women get the opportunity to learn from, grow and influence likeminded women across the globe, and foster lasting relationships.

Many of WAI Partners have also drastically changed their recruitment process, having more in depth interviews with women to uncover skills not listed in their profiles, and also listing only the 5 or so skills that are most important for the position.

WAI are passionate to have Members and Partners as Fans of Women in AI, actively empowering the community of women from school to university and other education, to have opportunities for networking and getting their dream jobs in AI in Private and Public sector or even create their own Start-ups. WAI Inspire Educate and Connect Women in AI with programs, and by speaking at events.

Join the Women in AI community as a volunteer, member or partner at www.womeninai.co.

WOMEN IN TECHNOLOGY



How to
BEAT
IMPOSTER
SYNDROME
as a WOMAN IN TECH

You may ask, “What is Imposter Syndrome? A state of mind that over 70% of men and women experience at some point in their lives.

Imposter syndrome refers to the persistent inability to believe that one's success is deserved or has been legitimately achieved as a result of one's own efforts or skills. It is the nagging feeling of inadequacy; an internal experience of incompetence within yourself, contrary to evidence and the positive opinions of others. While imposter syndrome is experienced by both genders, the term was coined by two female psychologists Pauline Rose Clance and Suzanne Imes who identified this in their 1978 research study on High-Performing Women.

Women in tech are susceptible to this due to the dire underrepresentation of females in the tech space. Furthermore, the skills, contributions and competence of women are often second-guessed resulting in self-doubt. A condition whereby the more she accomplishes, the more she feels like a pretender, unworthy, and inadequately skilled.

Gender diversity in the tech field is known to be insufficient. Over 50% of women leave the tech industry by age 35 according to research conducted by Accenture. 52% of them identify the lack of role models as a reason, while 51% mention company culture and inadequate support as contributing factors. Organisational culture can encourage pre-existing biases towards women, hampering their development and contributing to the feelings of imposter syndrome. Women experience this

inadequacy in confidence regularly.

Here are some tips on how women can overcome this syndrome and better advocate for themselves.

Know that Knowledge Gaps are not a sign of incompetence as some companies and colleagues may want to exploit a perceived lack of knowledge or experience. Rather, identify any gaps and work towards closing them continually as there is always room for improvement for everyone; male and female. Nobody can know everything; a desire to learn and grow constantly is a positive quality in the tech industry and work environment as a whole.

Remind yourself that you worked hard to be where you are. You deserve it regardless of you being at the right place, the right time and perhaps, you being a beneficiary of a gender quota policy.

Know you have unique skills and strengths. When a company hires you, you may not have the same qualifications or some abilities as another colleague, but you offer value. You bring your own experience and are unique – this makes you a good fit for your role.

Remember that your expertise is needed. When colleagues approach you with tough questions, needing assistance and solutions, it shows that you are a specialist and valued. Be encouraged

Talk about how you feel. Be open and honest about your worries to a mentor, friend, family member or therapist. This can help put it in perspective and alleviate anxiety.

Focus on your strengths. Don't look at what you can't do. Look to understand your unique capabilities and how to use them in the workplace.

“The skills, contributions & competence of women are often second-guessed resulting in self-doubt.

Keep your own achievements top of mind. Endeavour not to compare yourself to others and remember that success is all relative. Remind yourself of your achievements when you need a confidence boost.

If you think you are being discriminated against, experiencing gender bias and unfairly being made to feel inadequate or like an impostor, consider talking to HR or approaching the person making you doubt yourself. Call it out - don't let it go on unchecked. If you don't feel safe doing this, link with other women for advice and support. There are various organisations such as Women in Tech and Women in AI who can aid you.

It is important to protect your career progression as well as your mental health. Please pay attention to how you feel; and if the imposter syndrome is overwhelming you, do seek professional help from a therapist.



feature BETTY MBITHI

on CYBERSECURITY

📍 KENYA

According to ISC[1] research, the cybersecurity profession needs to grow by 5.4 million to close the global workforce gap.

I learned about cybersecurity for the first time through Cisco while working toward my CCNA (Cisco Certified Network Associate) certification. As a multidisciplinary field requiring the synchronisation of people, processes, and technology, I found it to be quite intriguing.

Being one of only three women in a class of 25 back then was one of the hardest challenges I had to overcome. At one time, I thought it was a “man” thing, but I persisted. I kept going because my mission was to prevent people's digital lives from being stolen or abused.

The upside is that I eventually overcame it, and my training center advanced and became a Cisco networking academy. This enabled us to offer a course in cybersecurity. It's inspiring to see so many young ladies in the industry. My goal is to use

mentoring to persuade as many women and girls as possible to work in the sector because they have a lot to give.

I continue to study because the security industry requires daily learning. To keep up with the most recent and exciting developments and to view the future from a different viewpoint, many people should focus on this area of professional growth. Emerging technologies offer significant chances for progressive changes.

You don't need to be tech-savvy to pursue cybersecurity. My background is not in technology, but I see that everything I do has a tech component, and as a result, I've developed a passion for technology. It doesn't matter whether you are female or male all that matters is that you have the knowledge, materials and people around you to inspire you. Don't ever stop trying; even if it is not for yourself, do it for others.

[1] <https://www.isc2.org/News-and-Events/Press-Room/Posts/2022/10/20/ISC2-Research-Reveals-the-Cybersecurity-Profession-Must-Grow-by-5-4-Mil-to-Close-Workforce-Gap>

SOUTH AFRICAN INVESTMENT FIRM TO PROVIDE GRANT FUNDING TO SUPPORT THE SWEDISH AI FUND'S PURPOSE OF PROVIDING FINANCIAL AID, GRANTS, AND SCHOLARSHIPS GLOBALLY TO THOSE IN THE AI INDUSTRY.

OAo INVESTMENTS *announces partnership with* **SWEDISH AI FUND**

OAO Investments, an investment firm shaking the South African investment landscape, announced its partnership with the Swedish AI Fund (SAIF). The partnership will fall under their technology pillar, OAO Technology. The partnership enables OAO Technology to identify best-suited candidates for funding through an evaluation process. This includes screening all applications, ensuring all due diligence processes are done and adhered to. Funds are thereafter released to successful candidates.

The fund will see the acceleration of Artificial Intelligence (AI) initiatives in Africa. It aims to drive awareness and enlightenment about the AI industry to the public, organisations, the technology sector, policymakers and governments who will be beneficiaries of a healthy AI industry. Only AI related programmes will be considered for funding.

SAIF is one of the multiple projects launched by the AICenter, a collaboration between several legal entities and experts towards a common goal: Equality, safety, and security in the AI industry. The AICenter founded in Sweden operates in 8 countries: Sweden,

Albania, Israel Germany, Georgia, South Africa and the United Kingdom. It cooperates with universities, leading companies and experts from the United Nations (UN) and The European AI Alliance.

AICenter, the founder of SAIF, enables and facilitates organisations, companies, and individuals to increase their business value and opportunities. AICenter also provides organisations with funding, certifications, guidelines, and certified training programs towards equality, safety, and security in AI.

In 2020 Sweden ranked number one in the Good Country Index (GCI) . The rank in the GCI motivated the AICenter to step into new terrain by facilitating funding through SAIF that aids the human race for a better future, a future with equality, safety, and security in the field of AI. "This partnership will aid our mission as OAO Technology, to accelerate the adoption of new technologies in Africa. The collaboration will contribute to the growth and development of AI on the African continent. We are grateful and look forward to serving our communities through this partnership" says Zamokuhle Aja-Okorie, Managing Director of OAO Investments.



MISSION TO ACCELERATE THE ADOPTION
OF NEW TECHNOLOGIES IN AFRICA