www.liquid.tech

The evolving Cyber Security threat in Africa

IT and financial decision makers respond to critical developments in South Africa, Kenya and Zimbabwe

August 2021

BUSINESS | CLOUD | CYBER SECURITY
HOME | LABS | NETWORKS | SATELLITE | SEA

AFRICA'S DIGITAL FUTURE

LIQUID
CYBER SECURITY

The evolving **Cyber Security threat** in Africa.

Cyber Security Report
August 2021

Contents

Executive summary

In July 2021, **Liquid Intelligent Technologies** (Liquid), a pan-African technology group, released the findings of its most recent research into **the evolving Cyber Security threat in Africa.**

Since the advent of the Covid-19 pandemic, **the threat landscape has changed dramatically.** This research investigates the evolving nature of the Cyber Security threat in Africa and how businesses in three key jurisdictions respond to it.

Liquid ran the research in **South Africa, Kenya, and Zimbabwe.** The sample included IT and Cyber Security decision makers across many sectors; including manufacturing, wholesale, retail, mining, and government.

The result showed that companies operating in these countries face **a notable increase in the frequency and sophistication of cybercrime.** The profile of the perpetrators has also changed from individuals to groups, organised syndicates, and even governments.

"Living in a digital era brings with it heightened threats for both businesses and individuals, and Cyber Security should now be at the centre of every business conversation."

Businesses in Africa are particularly vulnerable to cybercrime, with **more than half of the countries in Africa** having **inadequate Cyber Security laws and regulations,** making it a haven for cybercriminals. Companies operating in this environment face a dual challenge: lobbying governments for more stringent Cyber Security laws and protections, and addressing **the immediate threats** to their businesses.

This report examines the extent of the threats they are facing; highlighting the areas of most significant risk; giving insight into the impact that cybercrime, data breaches, and data losses can, and do have on companies operating in Africa; and **examines in detail what individual companies can do to protect their most valuable asset, their information.**

Introduction

When Liquid Intelligent Technologies (Liquid) published its first report on **Cyber Security and data protection** in Africa (2016), the world was very different. Since then, the Covid-19 pandemic has redefined how people in every country around the world live, work, and play. In Africa, ongoing challenges such as poverty, the impact of climate change, political uncertainties, civil unrest, and underdeveloped infrastructure add **additional layers of complexity.**

Within this context, the most reliable means of promoting broad-based development is to expedite universal internet access for all. Whether this is used to facilitate mobile banking for farmers in remote regions, deliver intuitive supply chain solutions for SMEs, or manage full-scale solutions for large corporations and financial institutions, **access to the digital economy** is fundamental to Africa's advancement.

"Securing universal internet access and the capability to operate safely and effectively within an increasingly digitised economy are the two of the greatest challenges for businesses operating in Africa today."

Also, with **remote working** now an entrenched operating model, businesses in Africa have the flexibility to compete on many different levels, whether locally, nationally, regionally, or internationally. As technology becomes more affordable, even micro enterprises can enter the digital space to compete on an equal footing with much more established businesses, regardless of geographic location.

Digitalisation is, however, a double-edged sword. As much as it brings an unprecedented platform for socio-economic development, it also carries **all the risks of operating in a digital environment,** including the risk of cyberattacks, data corruption, data breaches, and data loss.

This comes into sharp perspective when one recognises that **data is essential to the enablement of every business.** It is every business's most important asset and, even in small enterprises like spaza shops, it is **critical to decision-making.** The rapid move to cloud utilisation has only heightened the risk of both systems and data being compromised, bringing with it the need for **an entirely new level of Cyber Security.**

Technology and Cyber Security Trends in Africa

As in other jurisdictions around the world, Africa is facing a key trend in Cyber Security, namely the **increasing professionalisation of cybercrime.**

As one of the fastest-growing regions globally, the continent will have **1 billion internet users** by the end of 2022 (IT News Africa). As it is also the world leader in the use of **digital money transfers,** it is particularly vulnerable to cybercrime, especially as Cyber Security laws and regulations trail those in other countries significantly.

According to a report entitled Cyber Crime and Cyber Security Trends in Africa, published by Symantec in 2016, countries throughout Africa are facing massive socio-economic challenges and have neither the time nor the resources to focus on cybercrime. As a result, it is estimated that **more than half of the countries in Africa** have inadequate Cyber Security laws and regulations, making it a haven for cybercriminals. This is only exacerbated by the rapidly rising number of mobile phones in the region.

Weak and outdated security systems are estimated to cost the continent a staggering **USD4 billion** a year, so the time to take planned and concerted action to improve Cyber Security is now.

"We cannot afford to lose momentum when it comes to Cyber Security. If we do, Africa's growth trajectory will be severely compromised."

Technology and Cyber Security issues in South Africa, Kenya and Zimbabwe

In its latest survey into the digital landscape in Africa, Liquid delved into some of the most pressing technology and Cyber Security issues facing businesses operating in **South Africa, Kenya and Zimbabwe** today.

Methodology

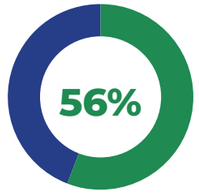
The sample comprised of **IT and Cyber Security decision makers** in various industries and sectors from manufacturing to communication, retail, financial services, construction, transport, and utilities in all three countries. Liquid identified all respondents as being leaders in their respective industries and sectors.

In South Africa and Kenya, the respondents were interviewed in groups, having agreed to be part of a permanent research panel and participate in research of this nature in the future. In Zimbabwe, respondents were interviewed telephonically and have also agreed to participate in future research.

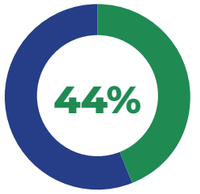
The sample size was as follows:

41	28	72	141
Kenya	Zimbabwe	South Africa	Total sample

The respondents' roles within their companies was as follows:



of the total sample comprised primary decision makers on Cyber Security issues.



of the sample comprised senior personnel directly involved in the Cyber Security decision-making process.

The objectives of the research were to:

- establish respondents' main concerns about Cyber Security threats to their businesses, selected from a list provided;
- establish the level of risk associated with remote working;
- establish the level of risk associated with the use of Cloud-based applications;
- establish whether the respondents' companies had or were planning to carry out Cyber Security risk assessments;
- establish whether Cyber Security is a budgeted item; and
- establish the greatest impact a security breach could or would have on the organisation, selected from a list provided.

Core issues

From the results of the survey, it is clear that the same **core issues** are of concern across the board. The most significant of these are:

53%
The safety, security, and protection of data

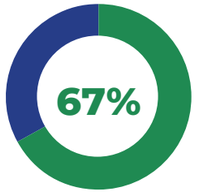
50%
The hacking of company databases

43%
Cyberattacks, including malware, phishing, and ransomware attacks

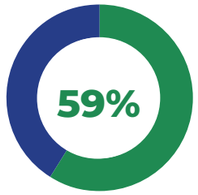
38%
The leaking, theft or loss of confidential client, company, employee, and customer information

Financial loss **(23%),** data loss **(20%),** business disruption **(15%),** and loss of reputation resulting from successful hacking attempts and cyberattacks.

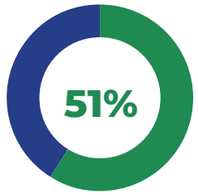
While the results of the survey differ from country to country, the most pressing Cyber Security threats were identified as:



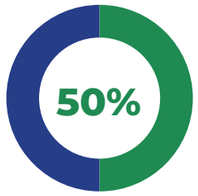
E-mail attacks, including spam, phishing, and social engineering attacks



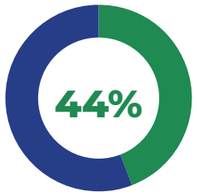
Data breaches, including data leakage, data disclosure, and data extortion



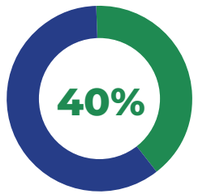
Web application and web-based attacks, such as the defacing of public-facing web sites



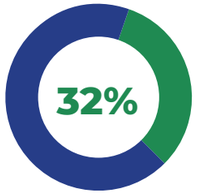
Malware attacks, including ransomware attacks



The security of confidential information stored in the cloud



Identity theft



Passwords being compromised

Another major concern is **shadow IT.** Also known as embedded, fake, stealth, rogue, feral, or client IT, this refers to IT systems, applications, and processes deployed in a decentralised way by individual departments or staff without the knowledge, input, or control of the centralised IT function. This is usually done to work around shortcomings within the centralised system but can create vulnerable back doors that provide easy access for bad actors.

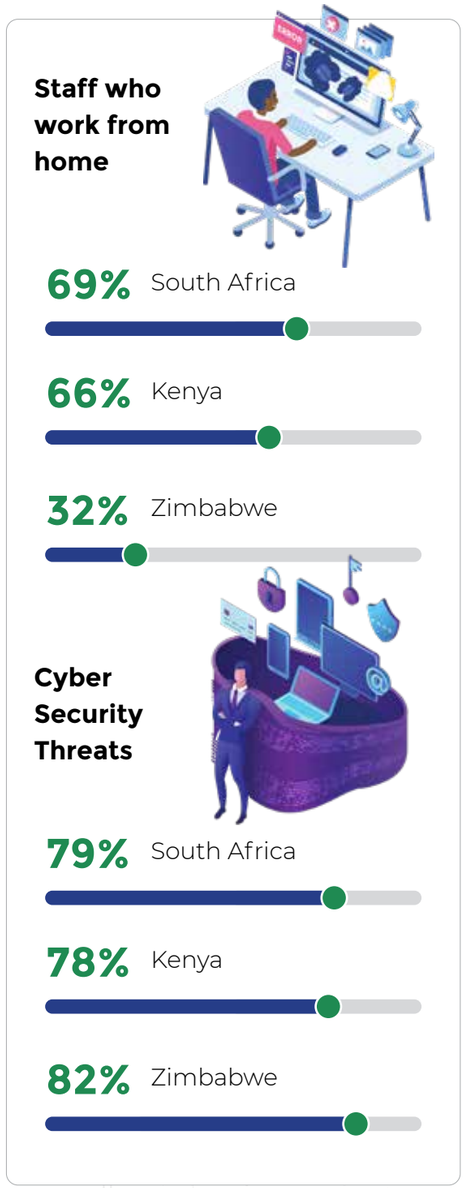
The risk of WFH

Perhaps the most significant Cyber Security risk that has evolved since the advent of the pandemic is the risk associated with the rapid shift to **working from home** (WFH). This is mainly because many staff had to be moved off-site at short notice when lockdowns were introduced, taking them **outside the control environment of centralised IT systems.**

Going on for two years since this shift, 69% of companies in South Africa and 66% of companies in Kenya indicate that most of their staff are still working from home. Only 32% of companies in Zimbabwe indicate the same, partly because of the country's more challenging environment.

Significantly, 79% of companies surveyed in South Africa, 78% in Kenya, and 82% in Zimbabwe indicated that they had experienced **an uptick in Cyber Security threats** over the past year, largely associated with remote working and the use of cloud-based apps, services, and storage.

The kind of **Cyber Security threats** experienced most frequently by these companies reflect management's concerns about key threat areas and are, in order of frequency:



- e-mail attacks, including spam, phishing, and social engineering attacks;
- malware attacks, including ransomware attacks;
- web application and web-based attacks;
- identity theft;
- data breaches, including data leakage, data disclosure, and data extortion;
- data breaches through remote working networks; and
- insider threats.

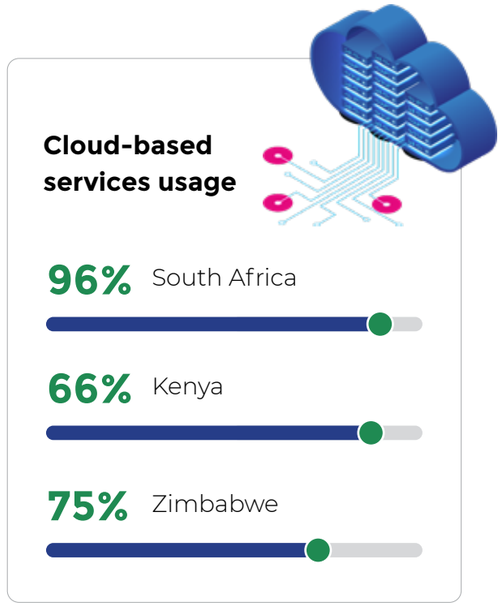
While some of these threats, like spam, phishing, and insider threats are well known and systems are protected against them, companies are less prepared for social engineering attacks, ransomware attacks, and cloud security breaches. And the enormous challenge of the day is to protect personal information against unauthorised sharing and hacking.

The risk of using Cloud-based services

The survey also indicated that 96% of respondents in South Africa, 95% in Kenya, and 75% in Zimbabwe use c**loud-based services** and acknowledge that this increases their **Cyber Security risk.**

The most commonly used Cloud-based services are:

- Microsoft Teams, Zoom, and Skype, platforms which are used to conduct online meetings;
- Microsoft Office 365, which is largely used for document creation, editing, and storage;
- Microsoft OneDrive, Dropbox, and Google Drive, which are used to store and share files online;
- Microsoft Azure and AWS, which are used for building, testing, deploying, and managing cloud applications and services; and
- Virtual Private Networks (VPNs), which are used to secure communications on shared and public networks.



Using Cloud-based services has opened up secure company networks to an entirely new set of risks. It has raised concerns about the **online exposure** of company information, customer and employee records, financial records and documentation, intellectual property, and proprietary systems and procedures. Another primary concern is the inability to control the security of information once it is in the cloud, potentially leading to **non-compliance** with legal and regulatory requirements.

A related issue is the lack of control over system features developed and owned by **third-party vendors**. This puts companies at risk of unprecedented price increases for the use of vendor services and, perhaps more importantly, at risk of a conflict of interest over the ownership of data hosted by the vendor.

Respondents identified the top five security concerns related to the use of Cloud-based applications as:

Loss of data and the inability to recover it

Managing user access to information

Visibility of and control over data

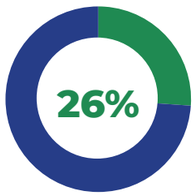
Lack of internal skills and resources to manage the risks associated with using third-party providers.

Compliance issues related to using providers in other jurisdictions

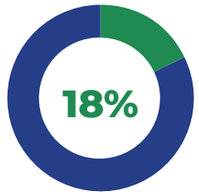
""Remote working and an associated increase in the use of cloud-based applications have created a new level of Cyber Security risk. Protecting personal information, as required by the Protection of Personal Information Act (POPIA), is an entirely different ballgame when played out in the cloud rather than in a secure, managed environment."

The impact of a Cyber Security breach

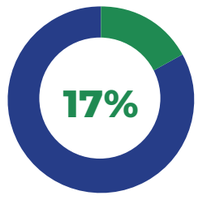
Respondents identified the following impacts of a Cyber Security breach as being of greatest concern to them:



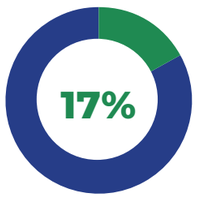
Financial loss



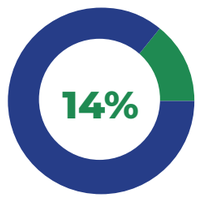
Loss of important company information



Reputational damage



Disclosure of strategic information to someone outside the business



Business disruption

Mitigation measures

With these issues in mind, many of the respondents indicated that they had put **additional Cyber Security measures** into place over the past year to protect their data assets and business continuity and reputation. In South Africa, 72% of respondents said they had done so, while in Kenya, this figure was 70%. In Zimbabwe, however, far fewer businesses had done so, with only 44% of respondents indicating that they had recently upgraded their Cyber Security measures.

In general, this increased expenditure was focused on safeguarding and protecting the company's data, securing financial transactions, preventing criminal activities such as fraud, preventing the loss of critical data, preventing the leakage of critical data to competitors, remaining competitive within an increasingly digitised operating environment, and securing profitability and business sustainability.

The **top mitigation measures** companies in all of the sectors surveyed have put into place are:

- advanced end-point threat protection (e.g., secure firewalls and application control software);
- end-point detection and response (EDR/MDR);
- e-mail content filtering and protection against malware;
- data loss prevention (DLP) measures
- continuous staff awareness training
- vulnerability management systems

Budgets for Cyber Security vary but, on average, account for 25% of total information technology spend.

"At the start of the pandemic, the big challenge in Cyber Security was to protect devices and systems as companies moved to remote working models. This issue has largely been addressed, and now the focus is very much on the security and protection of information."

What is important to note is that the Cyber Security focus has shifted significantly since the start of the pandemic. The objective is no longer simply to keep company networks safe but also to put adequate controls in place at the endpoints of the network, where the users are.

Ignus De Villiers
Head of Cyber Security

The Liquid Intelligent Technologies perspective

In a rapidly evolving digital and technology landscape, Cyber Security attacks are becoming more frequent, more sophisticated, and more challenging to defend against. This means that **Cyber Security should be at the centre of every business conversation** and should also be a top priority for individuals. From an organisational perspective, several key considerations need to be taken into account when protecting what is effectively every business's most valuable asset - its information.

A Cyber Security framework

Without exception, all businesses need to have a formal **Cyber Security framework** aligned to their strategy and objectives. Enterprises of different sizes have varying capacity and budgets, different information security requirements, face different threats, and have different legislative, regulatory, or industry requirements to comply with. They also have different people challenges, processes, IT footprints, services, and applications, so their Cyber Security frameworks need to consider all these factors.

There are many **best-practice frameworks and standards** that can be used as reference points. Examples include the ISO 27001 Standard, the NIST Cyber Security Framework (CSF), the CIS Top 20, the SWIFT Customer Security Program (CSP), and the IOSCO Cyber Security Guidelines. More specific industry-related solutions naturally must be considered when necessary, such as the PCI DSS and, of course, there are **legislative and regulatory requirements**, such as those outlined in GDPR and POPIA.

These frameworks and standards have a lot in common, so the challenge is to select what is applicable to and appropriate for the business. And that is just the first step.

Effective Cyber Security requires continuous management and improvement of the company's Cyber Security technologies and systems, so establishing an **information security management system (ISMS)** is a **critical first pillar** when putting a Cyber Security framework in place.

While the ISO 27001 Standard provides good guidance for implementing an ISMS, not all organisations can align with, adhere to, or comply with this standard. For those that are unable to do so, the following aspects need to be taken into account when considering an alternative:

Governance: The high-level objective should be to provide direction by establishing a strategy, policy, a supporting organisational structure, and management protocols to form the ISMS. Additional areas of importance are risk management assurance, compliance management assurance, continuous assessment of the effectiveness of security controls, and a planned process for continuous improvement. These are important not only for the **security of data** but also to assure **shareholders** that there are appropriate Cyber Security protections in place and that these are being overseen within the context of the company's corporate governance structures.

Risk: Risk needs to be managed consistently and effectively. An **information security and Cyber Security risk management methodology** is therefore essential. The objective of this is to identify and assess the risks to the business in these areas and to ensure that they are managed in line with its risk appetite. This methodology should include a **Cyber Security risk register** and a **risk mitigation plan.**

Compliance: Compliance with the legislative and regulatory requirements governing the business and the sector in which it operates is also essential. Compliance with POPIA is just one example.

People: It is vital for all staff to understand that they have a responsibility for Cyber Security and for those directly involved in this specific area of the business to have clearly defined roles and responsibilities. Acceptable-use policies and ongoing training and security awareness programmes are essential.

Process: Many Cyber Security processes are missing necessary steps that leave the business vulnerable to cyberattacks and the loss of critical information. Processes must be continuously checked and assessed regardless of the size of the organisation. One of the most important processes to have in place is an **information security and Cyber Security incident response process** with **supporting playbooks**. Also essential are standard operating procedures (SOPs) to ensure that security control effectiveness is measured to provide assurance to shareholders and other stakeholders.

Technology: Technical security controls and management protocols are also essential. These must be aligned to the risk mitigation plan and compliance requirements. It is generally good practice to have **a minimum-security control baseline** and add **advanced security controls** to address specific risk mitigation and compliance requirements.

The second critical pillar in any Cyber Security framework is a Cyber Security resilience control framework, enabling the ISMS.

This consists of the technical and non-technical security controls needed to meet the ISMS's objectives and provide resilience against Cyber Security threats. The following elements are required to establish an effective Cyber Security resilience control framework:

Identification: The system must identify **critical business functions** and **supporting information assets** that need to be protected in order of priority. It must also be able to identify weaknesses within the information system landscape.

Detection: It must further **detect anomalies and events** that indicate the possibility of a potential Cyber Security incident, which is essential to resilience. Early detection provides the critical lead time necessary to mount appropriate countermeasures against a potential breach and allows for the proactive containment of actual breaches.

Protection: The framework must also have effective security controls that protect information assets and services' confidentiality, integrity, and availability.

Response and Recovery: It is critical to respond immediately when an incident occurs. An **incident response plan** with **a team dedicated to activating it** is a fundamental requirement. In triggering a response, the team needs to refer to **documented playbooks** that are aligned to the threats most relevant to the organisation. Equally important is the ability to recover from the incident, for example, to recover data that has been compromised in a ransomware attack.

As standard practice, all organisations should have **offline backups** that are frequently tested to ensure their integrity. The same is needed to provide disaster recovery and business continuity. There must be formal, documented processes in place for backing up, testing and so on.

Testing: All elements and controls within a Cyber Security framework should be **regularly and rigorously tested** to ensure overall effectiveness.

Situational Awareness: Strong **situational awareness** can significantly enhance understanding and pre-empt cyber events and effectively detecting, responding to, and recovering from cyberattacks. A solid understanding of the threat landscape can help better identify and understand the vulnerabilities in critical business functions and facilitate appropriate risk mitigation strategies.

Learning and Evolving: it is essential to implement an **adaptive cyber-resilience framework** that evolves with the dynamic nature of cyber risks. This ensures the effective management of those risks continuously.

Technical baseline security controls

Getting the basics right is always important, especially when it comes to Cyber Security. The following functions should be part of the baseline security controls.

Concerning these functions, it is vital to consider consolidating options such as unified threat management (UTM) and unified security management (USM) or evolving technology options such as secure access service edge (SASE) and endpoint detection and response (EDR).

Many organisations assume that their baseline security controls are adequate, only to find that they are easily compromised. The best management protocol ensures that technical security controls are regularly **assessed by independent third parties** using pen testing, red/blue team testing, or tools that can do continuous validation, such as vulnerability assessment, breach and attack simulations, or automated pen-testing.

Advance technical security controls

Advanced security controls can and should be used to enhance resiliency. For example, signature-based malware protection is now not enough. More advanced options are necessary. These should also be capable of performing **behaviour-based malware protection** or **0-day protection** using sandboxing or something similar.

In the face of such a complex landscape, many companies are unsure as to where to start.

At Liquid, our advice would be to consider the **top Cyber Security threats** listed by entities such as ENISA and consider which of these are risks to your organisation. Of course, you may also need to consider advanced security controls to comply with legislation and regulatory requirements such as GDPR and POPIA.

It is equally important to consider the Cyber Security resilience control framework elements that have not been addressed. For example, a security incident and event management process or a security operations centre may be required to handle adequate situational awareness, or endpoint detection and response (EDR) may be needed to improve detection.

The following section offers some guidance as to how to respond to the **five most common Cyber Security threats**:

- **Malware, including ransomware:** Using only baseline security controls is an inadequate approach, so it is crucial to make use of the **advanced security controls** mentioned in the section above. A Defence-in-Depth strategy is required. This offers multi-level protection and covers attacks on endpoint devices (workstations, laptops, smart devices, removable media) and servers. It should also provide protection against the same risk with the use of groupware, such as Microsoft Exchange, also for email and web gateways, remote access, secure access service edge (SASE) deployments, as well as within collaboration tools. **Endpoint detection and response** (EDR) is now a must-have when it comes to protecting endpoints and servers against malware, and it also provides monitoring of these assets to prevent compromise.

- **Web-application attacks:** Effective baseline security controls are critical for public-facing web application services and the server OS instances they reside on. Public application server instances should be separated from data hosting or database server instances at the backend. Source code analysis and penetration testing of new or changed applications are always required before they go into production, especially if a **web application firewall (WAF)** hasn't been implemented to protect these applications. WAF solutions safeguard web applications against attacks such as SQL injections, X-site scripting and so on. It is important to remember that the amendment of default configuration settings, vulnerability management, and strong authentication are vital in securing public-facing web services.

- **Email, phishing, and impersonation:** A **secure email gateway or service** is critical to prevent phishing attacks, but it is equally important to **address the human factor** by doing security awareness training and phishing simulations, which teach users to handle such attacks appropriately. Impersonation protection is also advised, notably a solution in which DMARC checks are performed.

- **Identity theft:** Baseline controls are again critical. However, protection of user identities starts with having **identity and access management (IAM)** in place and even **identity and access governance (IAG) solutions** in more complex environments. Strong passwords are good but are no longer enough. Strong, **multi-factor authentication** is needed to protect user identities. It is also crucial to ensure that privileged user identities receive special attention. Hence, a **privilege identity management (PIM)** solution, which usually includes a password vault to protect service account passwords and enables privilege session control options, is advisable. It is also vital that **multi-factor authentication** is enabled for remote access solutions, as attackers have an easy way in via these solutions if they have managed to discover some user credentials and a password. Several attackers use weak Wi-Fi deployments to gain user credentials and passwords. It is, therefore, a good practice to **combine certificate and user authentication** when deploying Wi-Fi. Also, certificate authentication must be successful before user credentials can be requested. If necessary, an external service provider can be used to assist with these protocols.

- **Data Breaches:** Data breaches happen primarily because of ineffective baseline security controls, which enable attackers to gain elevated rights and then authorised access to data using compromised identities. Data breaches may, however, simply happen because laptops are stolen or lost. Data disclosure also occurs when removable devices are lying around and are not protected. To protect against data breaches within private networks, it is important **to enhance the native security capabilities of the underlying operating system (OS), unstructured infrastructures** such as SharePoint, or structured databases by using strong **encryption-based mechanisms** that are appropriate in the situation. Knowing where data is and where it is going cannot be emphasised enough, so mature **data leakage prevention (DLP)** and **cloud access security broker (CASB)** deployments are needed. Protection of data is complex, and third-party assistance is generally required to do it correctly. Further solutions to consider are digital rights management (DRM), data classification and labelling tools, data access governance, and data discovery tools, as well as email encryption and archiving. **Offline backups** of critical data are a basic necessity, especially when recovery is required.

- **Denial of Service:** **Distributed denial of services (DDOS)** solutions, including scrubbing or similar, are required for those businesses for which the availability of their public services is essential. Consideration should, of course, be given to where such services must be located, whether on-site or in the cloud.

Security by design

Security by design principles is key when implementing a Cyber Security resilience control framework. This means building a **minimum attack surface area** using approaches such as Zero Trust, securing default settings, hardening the underlying infrastructure, applying the principle of least privilege, establishing defence-in-depth, implementing fail securely, separation of duties, and so on.

There are many factors to consider. If a business does not have the capabilities to protect itself against cyberattacks, data losses, and data breaches internally, it should consider involving a suitable Cyber Security provider to assist. Skilled staff and the services of trusted service partners are indispensable to protect data assets.

Conclusion

Experts agree that **Africa has a long way to go in terms of Cyber Security,** acknowledging that improving laws, regulations, infrastructure, and systems are essential to prevent cybercrime and sustain socio-economic growth.

Many countries, including Kenya, Nigeria, Ghana, and Uganda, have experienced enormous difficulties with cybercrime. This affects many industries and sectors, but banking and financial services, e-commerce platforms, telecommunications, and government services have been particularly hard.

In August 2021, Cyber Security firm Kaspersky reported that four countries in Africa – South Africa, Kenya, Nigeria and Ethiopia – had been the subject of **85 million malware attacks** in the preceding six months, with South Africa accounting for **32 million** of these. This indicates that cybercriminals and hackers continue to focus on Africa, where controls are known to be weak.

While malware has always been an important issue, this spike in activity highlights that **hackers are doubling down on their efforts to compromise consumer and corporate systems** and gain access to critical data and information.

The need for companies operating in Africa to protect their systems and data is therefore urgent.

Given the current legislative and regulatory environment, they need to adopt a **two-pronged approach.** Firstly they need to adopt **best-practice Cyber Security mitigation and management protocols** to protect their businesses against sophisticated cybercriminals who operate in jurisdictions around the world have identified companies in Africa as being particularly vulnerable to attack. And secondly, just as importantly, they need to adopt **continuous training and awareness programmes** within their organisations to protect against vulnerabilities and threats from within.

*"At **Liquid Intelligent Technologies,** we believe that the first step to ensuring a secure digital environment is training employees so that they can safely navigate and grow in a digital-first world. This enables us to deliver the 'secure people' aspect of Cyber Security as confidently as we deliver every other component of our Cyber Security solutions."*

To find out more about what Liquid Intelligent Technologies can do for your business, visit us at

www.liquid.tech

or contact us on the following

LinkedIn 

Facebook 

Twitter 

Email