www.liquidc2.com

The Evolving Cyber Security Landscape in Africa.

Cyber-attacks, hacking, data loss: Decision-makers across South Africa, Kenya and Zambia share their cyber security concerns.

Liquid C2 Cyber Security Report 2022

CLOUD | CYBER SECURITY | EDGE

WE'LL C2 IT.

LIQUID
CLOUD & CYBER SECURITY

Contents

Executive summary

Throughout 2022, Liquid C2, a business of Liquid Intelligent Technologies, a pan-African technology group with extensive cloud and cyber security expertise, collated its research, analysis and findings around Africa's evolving cyber security threat.

These findings, gleaned from discussions with decision-makers across South Africa, Kenya and Zambia, highlight a landscape fraught with complexity, increasingly challenging threat actors, and a sharp increase in organisational awareness.

In the past, cyber security has battled to gain traction and visibility at the boardroom table. Considered a grudge purchase with a hint of hysteria, it was relegated to a box-ticking exercise with limited resources that impacted efficiency. Today, the picture is very different. Decision-makers have become increasingly focused on risk mitigation strategies, cyber security investments and robust policies designed to ensure that their organisations don't fall victim to a threat that's become both virulent and sophisticated. The research found that there has been a significant change in how decision-makers perceive cyber security and how it has become one of the organisation's top priorities, with Kenya showing the most marked shift in awareness overall.

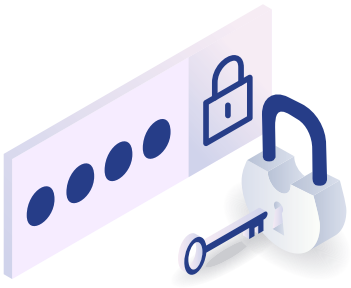
*This shift has been driven by the **radical change in working frameworks** from in-office to online during the pandemic to a hybrid approach that's gained traction over the past two years. **An increasingly dispersed workforce** has put immense pressure on cyber security teams.*

From ensuring the protection of one environment for hundreds of employees in the office, they are now tasked with protecting hundreds of environments scattered across different countries, geographies, time zones and regions.

Most of those surveyed in South Africa are in a hybrid stage; Kenya has a significantly smaller percentage of companies adopting a hybrid model, while most are either fully remote or in the office, and Zambia has little to no remote working.

One of the primary threats cited by decision-makers around remote and hybrid working was authorised use – the concern that the person accessing the device or the company resources is not a family member or someone misusing company-owned resources. There are concerns around managing this challenge alongside malicious code from harmful websites and lost or stolen devices. Companies are therefore focusing on security solutions that help them manage these challenges more effectively, such as endpoint protection, firewalls, and backups. Two-factor authentication has increased while staff awareness and training remain low.

Hacking** is the leading concern for companies in South Africa, with Kenya and Zambia, showing an increase in their concerns around this threat, while email attacks and social engineering attacks are still perceived as **two of the biggest ongoing threats.



"Software compromise due to **vulnerability exploits, theft of company information,** and **non-compliance** are no longer cited as the issues that would have the biggest impact on a business in the event of a cyber security breach in 2023, a significant change from 2022. This could be because companies believe that the measures they've put in place are **enough to mitigate** or **reduce these threats**"

Password compromise is a rising concern in South Africa and Kenya. At the same time, Zambia is concerned about social engineering attacks, and all three countries have shown increased awareness around the risks presented by SMS attacks. However, this remains a low priority overall.

All three countries emphasised that loss of reputation, financial impact and business disruption were their primary concerns around a successful attack. What is interesting is that all countries showed a marked increase in their belief that they have done more to embed security than in the past - they are aware that more attacks are on the horizon but feel that their cyber security posture has been enhanced accordingly. However, as security is a moving target, most companies have continued investing in cyber security solutions that consistently improve their security posture. Business continuity and partnering with cyber security service providers remain a high priority in South Africa and Kenya but low in Zambia

*The changing benchmarks of cyber security, the increased sophistication of attacks, costs and the ongoing talent shortage are the **key factors** driving the move towards outsourcing cyber security to **third-party security service providers.***

Regarding cloud investment, Microsoft remains the dominant cloud-based platform in use across all three countries. However, South Africa has the highest adoption, while Google is gaining traction in Kenya and Zambia, with smaller companies looking to adopt this platform in South Africa. This is driven by cost and accessibility, and perceptions around security.

This report digs into these threads and trends to examine the threats, challenges, perceptions and methodologies adopted by South Africa, Kenya and Zambia as they manage the evolving cyber security threat on the continent.

It highlights the areas of significant risk, provides insight into the impact of cybercrime, and focuses on what companies can do to protect their assets, systems, employees and information in 2023 and beyond.

Introduction

Since Liquid C2 published its first Cyber Security and Data Protection in Africa report in 2016, there have been radical changes in both workstyle and security threats. It was a different world, one that the COVID-19 pandemic and the dramatic evolution of digital platforms, services and solutions had not fundamentally reshaped. In Africa, the additional layers of complexity introduced by political uncertainty, economic variability, ageing infrastructure and poverty continue to influence how organisations operate and invest in the future.

Within this context, this report looks at some of the key trends that have emerged over the past six years in Africa, specifically with regard to cyber security and cloud services investments and strategies. Interviewing decision-makers and

IT professionals across South Africa, Africa and Zambia, the report sifts through the data to reveal an increasingly aware and sophisticated landscape plagued by inconsistencies and socio-economic challenges. The sample profile across all three countries primarily came from banking and finance, education, manufacturing, mining and quarrying, construction, communication, wholesale and retail trade.

*The **focus of the research** in this report is to establish how this **evolving threat landscape** has changed **how organisations approach their security** and the main concerns that decision-makers have around these **cyber security threats** to the business.*

It unpacks the perceived impact of a breach, the most significant cyber security threats, how prevalent they have become, and what solutions and services companies rely on to manage and mitigate them. In addition, it looks at how remote and hybrid working influence cyber security strategies, what impact working from home (WFH) has had on the organisation, and how WFH has changed the type of threat actor and the threats themselves.

*The analysis within this report looks at how companies **leverage cloud-based services** and their evolution alongside the cyber security landscape. It also details **how decision-makers feel** about using **cloud services** within this challenging landscape, what their primary security concerns are, and what impact these concerns have when it comes to their **cloud adoption strategies.***

The report unpacks how it has become critical for companies to understand how security intertwines with digital transformation and adoption strategies. Cost and talent are two key issues that affect how organisations approach their cloud and security investments. The cyber security skills gap continues to inhibit the organisation's ability to access skilled talent, not only in terms of finding the talent but also affording it. Experienced cyber security professionals are hard to find and expensive to retain. This cost factor is carried over into how companies approach their security spend per employee and select cloud services. Companies are looking for solutions to remain competitive and agile without compromising their cyber security resilience and capability.

Cyber security trends in Africa

Over the past three years, the Liquid C2 Cyber Security Report has analysed the key concerns and challenges facing organisations regarding the cyber security threat and revealed how attitudes and approaches have changed alongside increasingly voracious cybercrime methodologies and attacks. Perhaps the most interesting trend is the radical drop in how companies perceive their security measures.

A more confident stance

Organisations have regularly placed 'inadequate security measures as one of their most prominent cyber security concerns, but in 2022 this dropped dramatically.

In 2021 and 2020, hacking, email and data protection were the dominant concern, with most citing that it was important to put measures in place to protect data and systems. This dip in concern is aligned with the fact that companies have put measures in place to combat cybercrime and their belief that these mitigations are significantly reducing the risks. This belief is echoed in the shift in perception around what impact a cyber security breach would have on the business – on the whole. Organisations are less concerned about business disruption, loss of data, and damage to reputation than in the past.

Interestingly, while organisations feel confident in their security mitigation processes and investments, they have highlighted a growing concern around email attacks, data breaches and malware. This is a conflicting perception – on the one hand, companies know that the threats have become more sophisticated and capable, but on the other, they believe they've done enough to protect against them. The reason for this conflict is that they feel they have done more to support security than in the past but are aware that there remain threats that they should be concerned about that may yet result in significant business impact in the future.

However, the key trend here is a markedly increased focus on risk mitigation and security investment that aligns with the emerging second trend.

Security has become a boardroom priority

Another thread that has emerged over the past year is around the perception of a cyber security threat. In the past, cyber security has been relegated to IT and reluctantly allocated budget as a grudge purchase forced on the organisation by hype. Now, companies recognise the severity of the threat – as reflected in the increased investment into security solutions and systems – and are putting far more controls in place.

Over the past three years, there has been a significant increase in how they approach their investment into cyber security controls, the types of threats that could have the most impact on the business, and the evolving nature of the cybercrime landscape as a whole. Email, phishing, spam, data theft, data leakage, data breaches, ransomware, and malware have gained traction as the most significant concerns facing organisations and has driven an increased focus on investing in security services and solutions that will reliably mitigate these concerns.

Decision-makers are also paying more attention to security and IT teams, particularly when it comes to the evolving nature of the threat landscape. On one side, those responsible for cyber security are concerned with how cybercriminals and their methods are constantly evolving and innovating – the attacks are intelligent, sophisticated and leverage next-generation technologies such as automation and artificial intelligence (AI). This puts immense pressure on security to stay ahead of the threats, a pressure that's only growing in light of legislative and regulatory requirements increases.

Regulatory pressures are changing business approaches

While regulation and legislation differ significantly across the three regions surveyed in the report, it remains a growing challenge. Companies must comply with regulatory expectations and ensure their security protocols and parameters align with local and global expectations. This drives cyber security awareness across the organisation – from the C-Suite to security teams and employee security training.

Skills have become a priority

Human error remains a substantial contributing factor to security breaches. The so-called human firewall is often the weakest point in the organisation's defences due to poor training and awareness. This was a trend driven by a lack of internal awareness and executive commitment and is now undergoing a significant shift. Employee awareness and training are rising, with many companies investing in cyber security programmes designed to simulate the most prevalent attacks.

This is perhaps one of the most important trends to emerge over the past three years, as employee awareness remains one of the most effective preventative measures. Leaders must stay focused on embedding security training and understanding within the organisation, as this is one of the most effective approaches to reducing the risk of a successful attack and potentially impacting the organisation's security posture.

On the other side of the skills development coin is the trend that hasn't gone away – cyber security talent. This challenge has worsened as the shortage of skilled security personnel continues to impact the business and its ability to hire and retain cyber security professionals. This has led to a marked shift from in-house security teams to third-party security service provision as companies look to provisioned teams to fill the gaps.

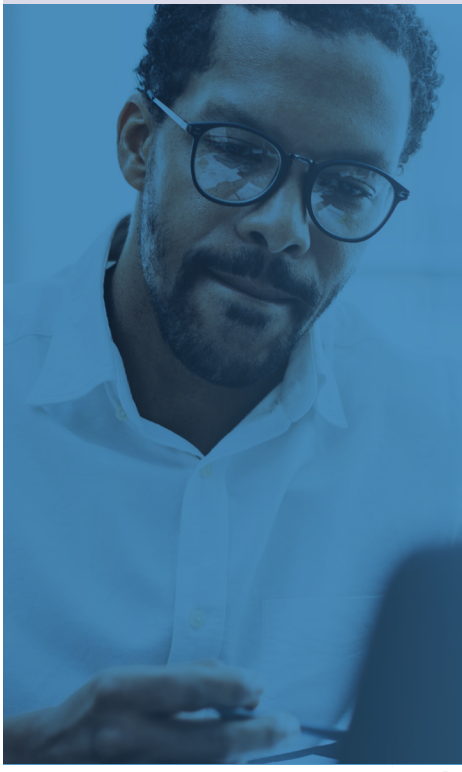
Cyber security is now seen as an enabler

The impact of cyber security is felt across any organisation of any size. A successful attack can bring down Goliath as easily as David. This makes the investment into a robust and capable security posture as much an enabler as an expense. It allows companies to expand their digital foundations, explore new markets and opportunities, and build customer relationships with confidence. This, perhaps more than anything in the Age of Information, is critical to business longevity.

Moving forward...

Organisations need to remain vigilant. Cyber security threat actors are intelligent and capable, their engineers committed to the profits generated from extortion, fraud and data theft, which means they are constantly evolving their approaches to overcome next-generation security measures. As a result, companies cannot afford to rest on their laurels – they must evolve alongside the cyber threat and consistently invest in the right tools, training, and service providers.

Managed security services (MSS) remain a trusted and capable resource for organisations looking to embed security throughout the business. In addition to providing the business with access to extensive expertise and skilled security talent, these companies help organisations effectively bypass the risk of outdated security or unexpected vulnerabilities by remaining ahead of the threats, understanding the trends and providing constant vigilance.



"Cyber security is an **enabler for the business.** If you understand the threats and the risks you're facing, then you're already ahead of the game. And remember, if your business is hacked or compromised, this will **impact how customers perceive you** and the amount of trust they give you. You can operate confidently if you're compliant, committed, and cyber-secure".

Methodology and objectives

In the third edition of the Liquid C2 Cyber Security Report, the research delved into the most pressing technology and cyber security issues facing South Africa, Kenya and Zambia organisations.

Methodology

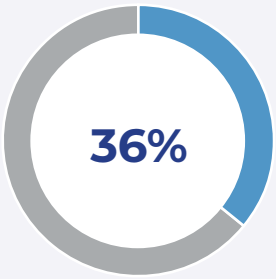
The sample comprised IT and Cyber Security decision-makers across multiple industries and sectors, and all respondents were identified as leaders in their respective industries and sectors. To participate in the survey, respondents had to be a decision-maker around cyber security issues, work in the research and development (R&D) department, and play a significant role in cyber security planning and investments.

The sample size for 2022 was:

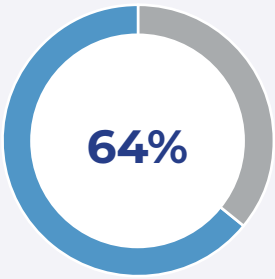
70	40	29
South Africa	Kenya	Zambia

In South Africa and Kenya, the methodology for this study was to interview respondents on a research panel and have agreed to participate in research panels on an ongoing basis. In Zambia, the respondents were interviewed over the phone from a list provided by Liquid.

Respondent roles:

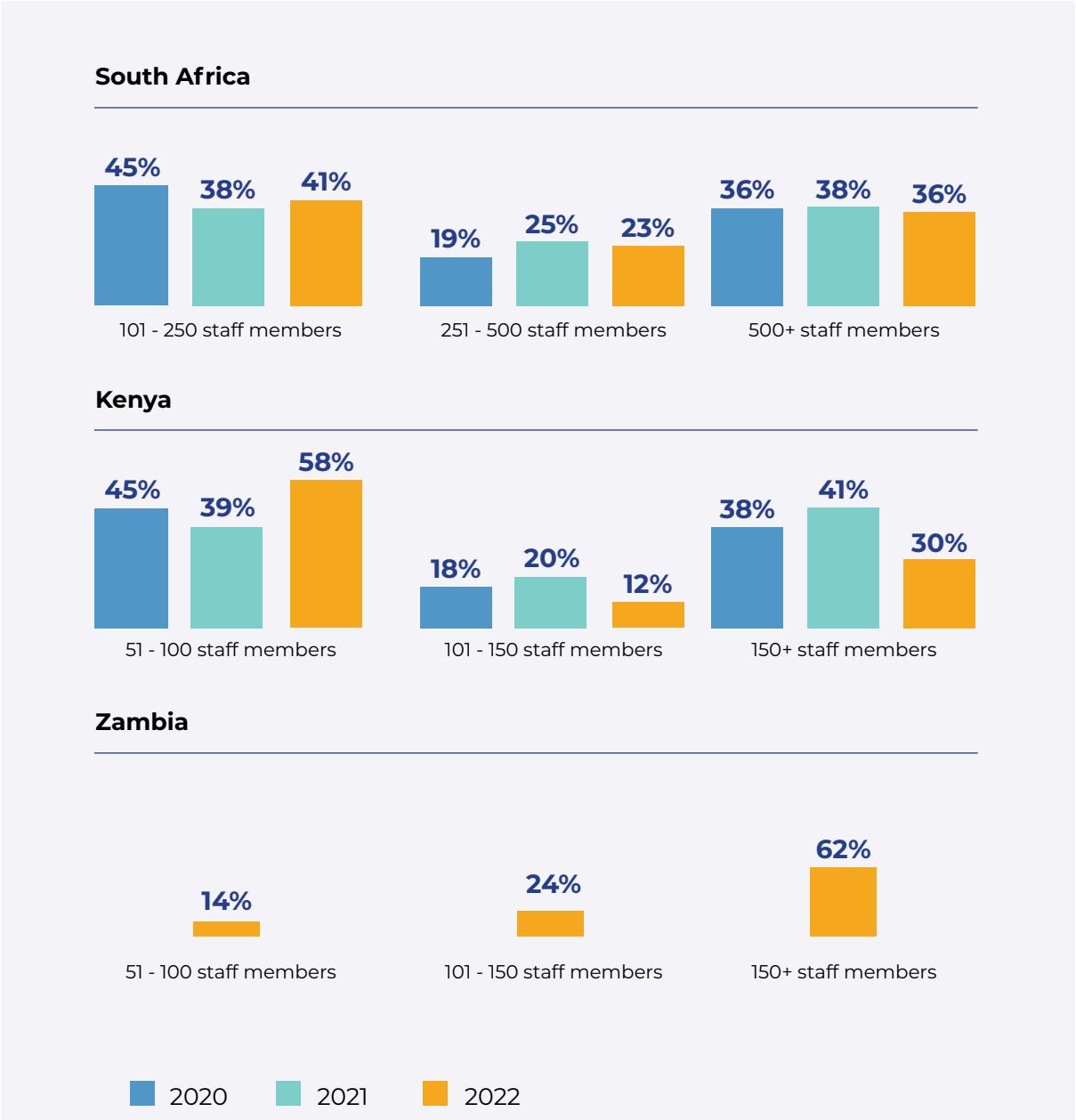


I am a decision-maker on cyber security issues and work in IT



I am involved in all decisions around cyber security issues and work in IT

Company size:



Total Sample n=139 | (2021, n=141 / 2020, n=109)

South Africa
n=70 (2021, n=70 / 2020, n=69)

Kenya
n=40 (2021, n=41 / 2020, n=40)

Zambia
n=29 (New country in 2022)

Industry Sector:

The sample profile predominantly lay across the following sectors:

In addition, it included respondents from wholesale and retail trade; transport and storage; electricity, gas and water; motor trade and repair services; tourism; agriculture; and betting and gaming.

The Research Objectives

The primary research objectives of this report were to establish:

The primary concerns that decision-makers have around the cyber security threats to the business;

The biggest impact a breach could have on the organisation;

The most significant cyber security threats to the business;

If there has been increased cyber security threats and/or data breaches;

What cyber security controls, safeguards and services organisations use.

The research also undertook to unpack the cyber security perceptions around remote working. To this end, it focused on:

Degree of concern about cyber security breaches as a result of working from home (WFH).

Breaches that the organisation may have had as a result of WFH.

Types of breaches that are perceived to be a result of WFH.

Interventions put in place to prevent WFH cyber security breaches.

Cloud remains a priority investment for organisations, particularly in light of its ability to enable business productivity and growth. To this end, the report also focused on:

What cloud-based services were organisations using?

What security concerns do organisations have around cloud-based services?

Understanding the key elements of their cloud adoption strategies.

In addition, the report looked at the following key issues and trends:

The cyber security skills accessed by the organisation.

What frameworks had been put in place to improve cyber security resilience?

The percentage of IT budgets allocated to cyber security.

The claimed budget spend per employee.

Demographics of the organisation, including size, industry, sector and respondent level.

Core issues

The survey results across the different research objectives found critical issues across the board. The most significant of these are:

68%

Think hacking and unauthorised access are the biggest cyber security concerns for the business

21%

South African organisations perceive that the biggest impact of a cyber security breach is on finance.

20%

Kenyan organisations perceive that the biggest impact of a cyber security breach is reputation.

74%

Think email attacks, including phishing and spam, are the biggest cyber security threats.

30%

Zambian organisations perceive that the biggest impact of a cyber security breach is towards business disruption.

60%

Think the most concerning business risk is the illegal company or client information access.

76%

Believe that cyber security threats have increased over the past year.

58%

Have experienced increased data breaches.

61%

Have experienced increased data breaches from remote and hybrid working.

72%

Have implemented advanced endpoint protection to mitigate the cyberthreat for remote and hybrid working.

83%

Are considering business continuity services.

68%

Have appointed cyber security staff or signed up with a cyber security team over the past year.

65%

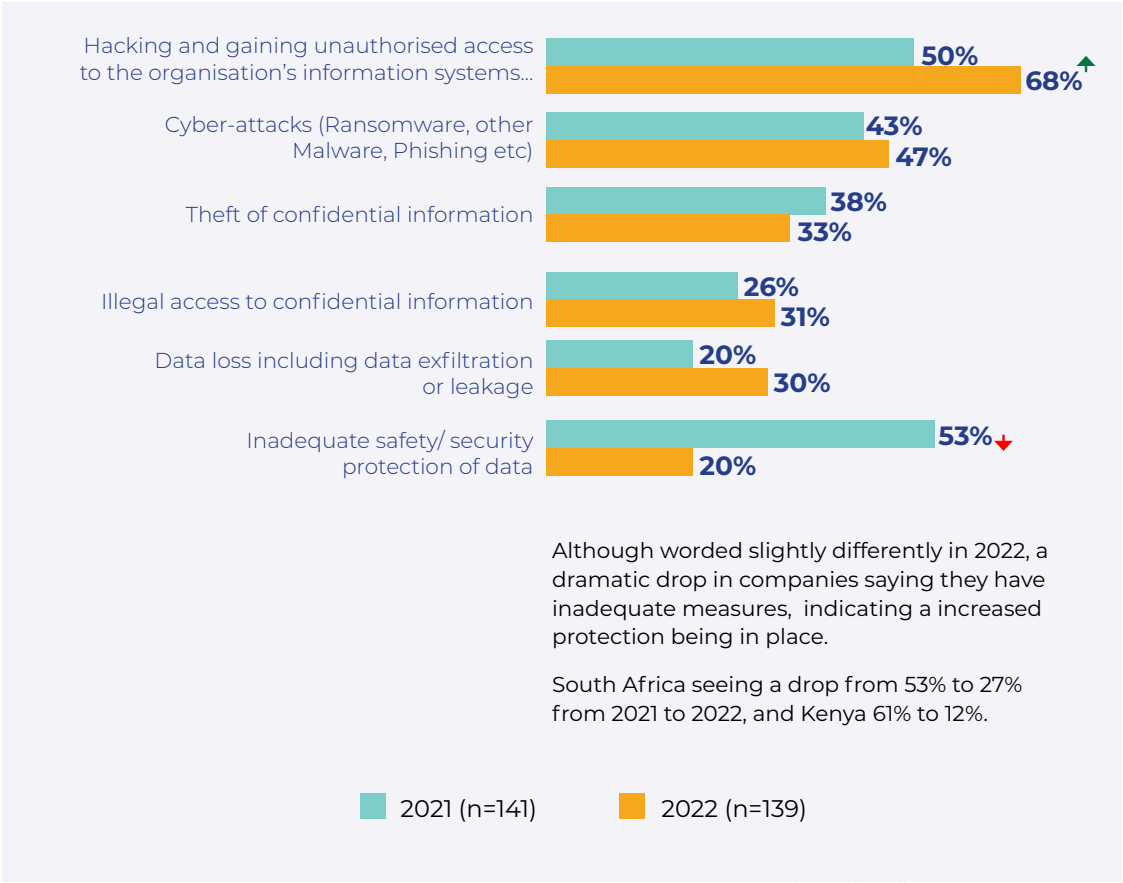
Have a digital adoption strategy and roadmap for the next two years.

Perceptions: threat and risk

The report found that organisations perceived hacking and gaining unauthorised access as the leading concern around cyber security.

This is followed by cyber-attacks, illegal access to information, and data loss, including exfiltration or leakage. Hacking has remained a concern over time but has seen a significant increase, particularly in South Africa and Kenya, where it has almost doubled over the past year from 41% in 2021 to 72% in 2022. It's the top risk cited by Zambia (62%), but it isn't given as much weight as the other two countries, likely due to South Africa and Kenya being further down the road in developing their cyber security safeguards and understanding. Zambia also puts cyber-attacks at the bottom of its perceived risks, while South Africa and Kenya have it in second place.

Hacking has seen a significant increase, particularly in South Africa and Kenya, where it has almost doubled to 72%.

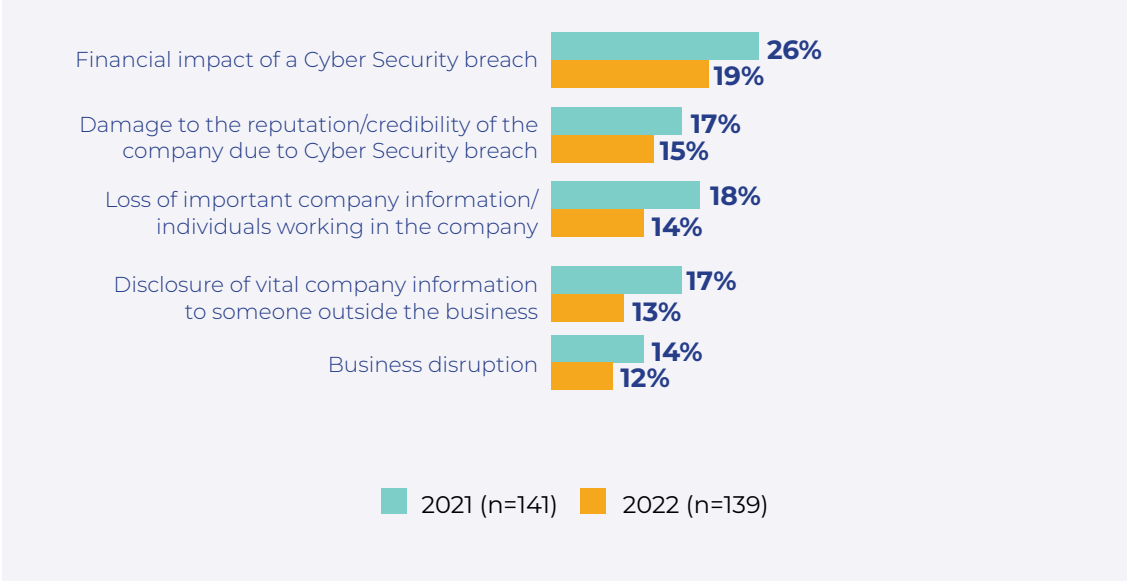


> ***Email attacks that include phishing and spam have increased to 74%.***

However, perhaps the most startling result is that there has been a drastic drop in how companies perceive their data's safety, security and protection. For example, in 2021, 53% felt that their protection measures were inadequate, but in 2022 this dropped by 33%, with only 20% citing this as a concern.

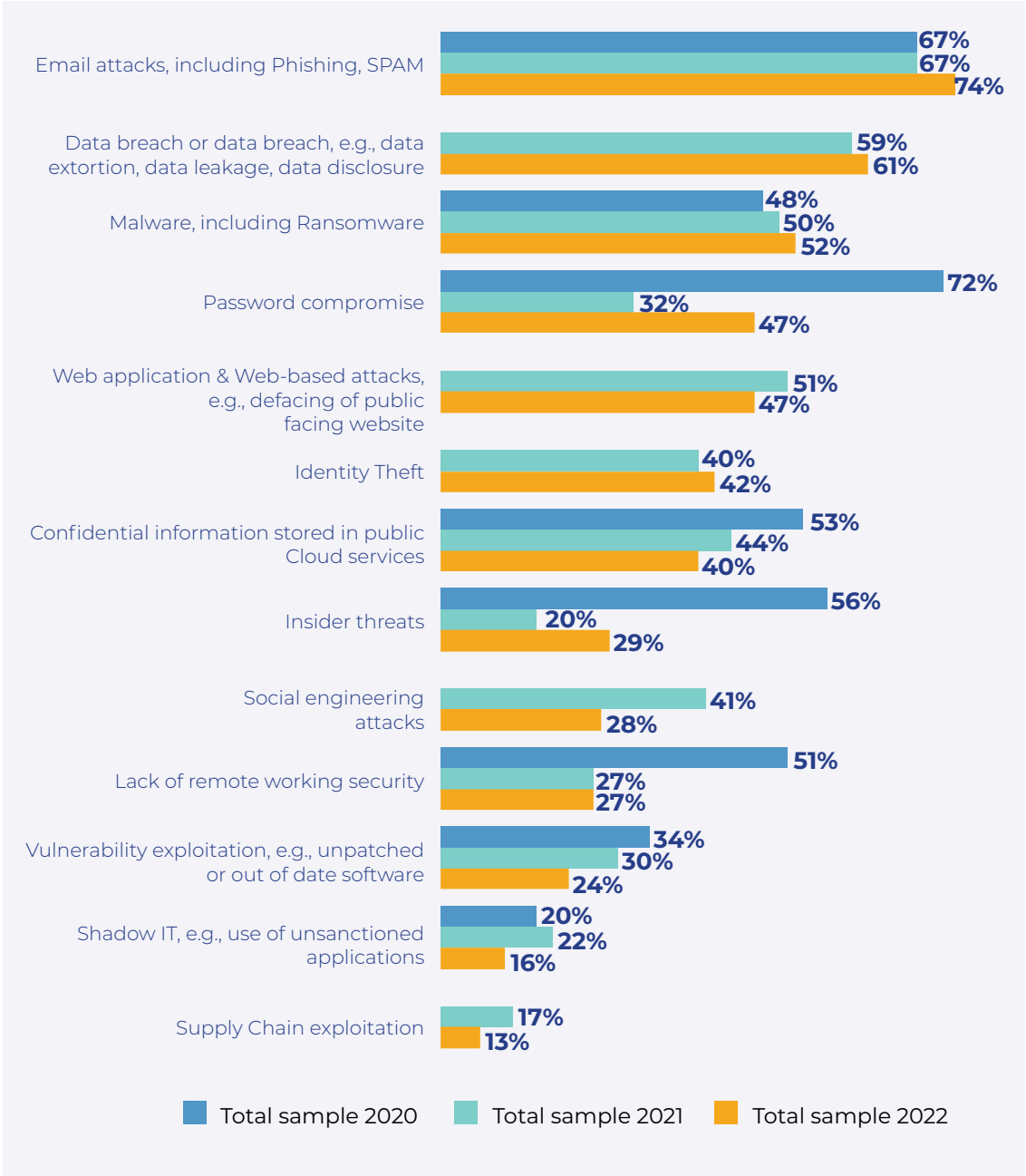
Overall, most countries feel that the most significant impact a cyber security breach would have on the business is financial. Still, South Africa prioritised this at 21% compared with Kenya prioritising damage to reputation (20%) and Zambia prioritising business disruption (30%). Across all three countries, financial impact, damage to reputation and loss of important company information were the top three concerns. Reputational damage remains a significant concern across all countries, and when it comes to the most significant cyber security threats to the business, there have been significant changes in perception compared to 2020 and 2021.

Email attacks that include phishing and spam have increased to 74% compared with 67% in the previous years, while data breaches that include data extortion, data leakage and data disclosure have risen to 61% compared with 2021's 59%. In third position, malware has risen from an average of 49% to 52%.



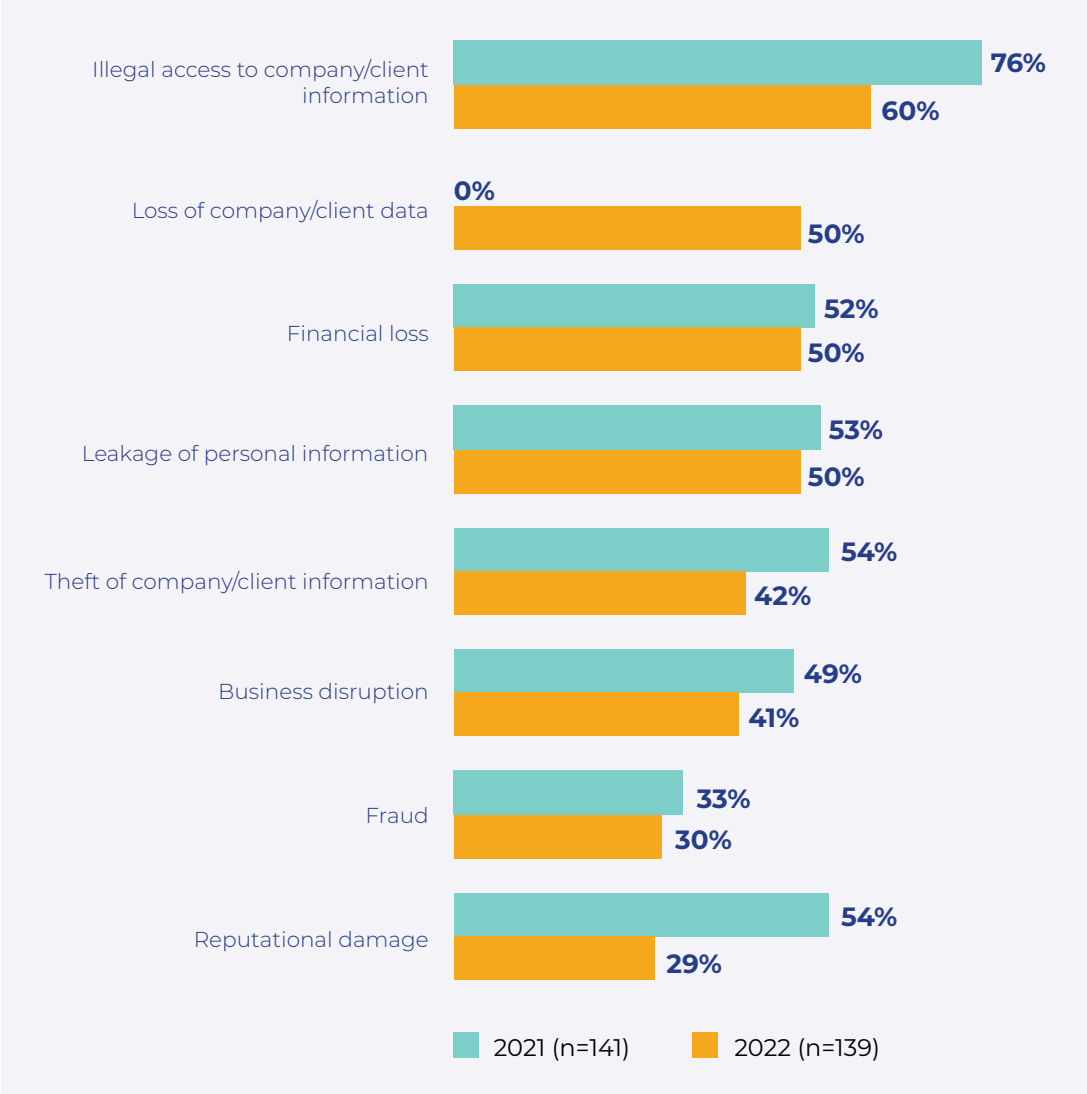
Companies are far more concerned about malware, email and data breaches than ever before; this is reflected in how different countries are affected by cyber threats.

South Africa, for example, continues to have the highest incidence of targeted ransomware and business email attacks of any African country, according to Interpol's African Cyberthreat Assessment Report 2021, and this is reflected in the research.



The illegal access to and theft of company and client information remains the most concerning business risk in the event of a cyber security breach (60%), although this has dropped significantly from 2021 (76%). The loss of company and client data has risen to second place at 50%, while financial loss remains relatively steady at 50%. Interestingly, business disruption, the theft of client or company information and reputational damage have dropped dramatically compared with previous years.

***The loss of company and client data* has risen to second place at 50%, *while financial loss remains relatively steady at 50%*.**



This is reflected in the perception of cyber security threats. Across South Africa (77%), Kenya (82%) and Zambia (62%), decision-makers believe that cyber security threats have increased over the past year, with email, data breaches and malware cited as the most pervasive.

Unfortunately, the perceptions are aligned with reality, with a significant number of companies having experienced an increase in data breaches. The overall total of

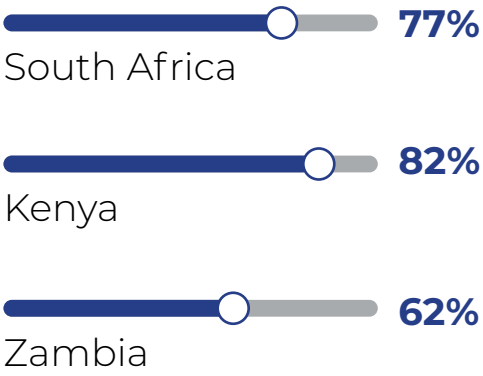
companies that have had a breach in the past year is 58% which is aggregated from South Africa (56%), Kenya (90%) and Zambia (17%).

The Remote Risk

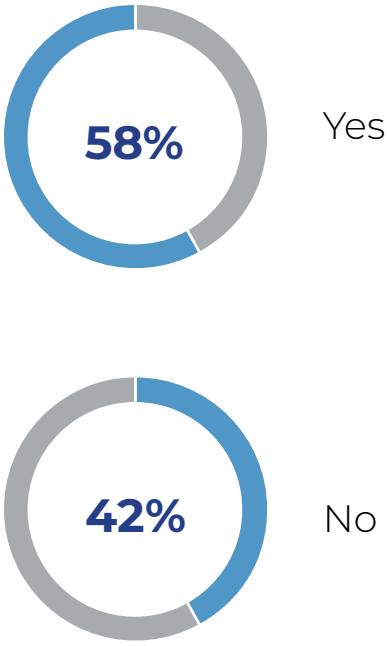
Of course, remote and hybrid working have played no small role in the threat landscape. Security is spread thin across multiple locations, employees remain the weakest security link, and unexpected vulnerabilities put the business at risk. The research reflects these challenges, with 61% of companies citing remote and hybrid working as the direct cause of a successful breach or as the leading risk factor when mitigating the security threat.

Across all three countries, around 43% operate a hybrid model, 14% are remote, and 43% are in the office. The most significant risk comes from email, which has become increasingly sophisticated and more pervasive thanks to WFH and hybrid working frameworks. The primary concern with email is how people work and use their devices and systems.

Perception of Security Threats:

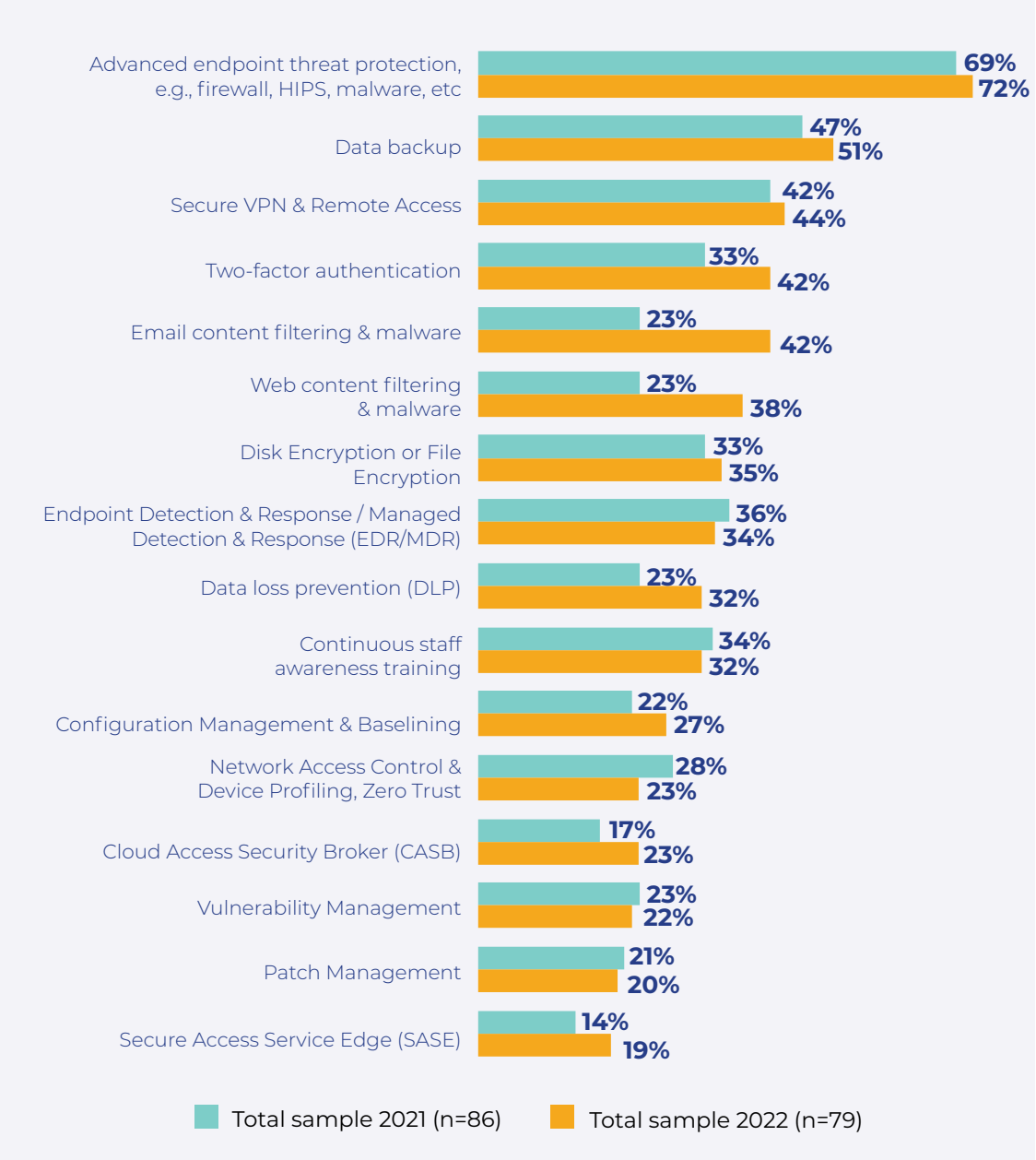


Have there been data breaches in the last year?




Email attacks, including Phishing, SPAM
67%
Password compromise
48%
Data breach and data theft, e.g. data extortion, data leakage, data disclosure
44%
Malicious code infections when visiting know bad Web sites
40%
Unauthorised use, e.g. family members misusing company owned resources
35%
Social engineering attacks
31%
Malware, including Ransomware
31%
Confidential information stored in public Cloud services
31%
Identity Theft
29%
Lost and stolen laptops
29%
Vulnerability exploitation, e.g. unpatched or out of date software
21%
Shadow IT, e.g. use of unsanctioned applications
17%
Organisational information not backed-up frequently
17%
Other
2%

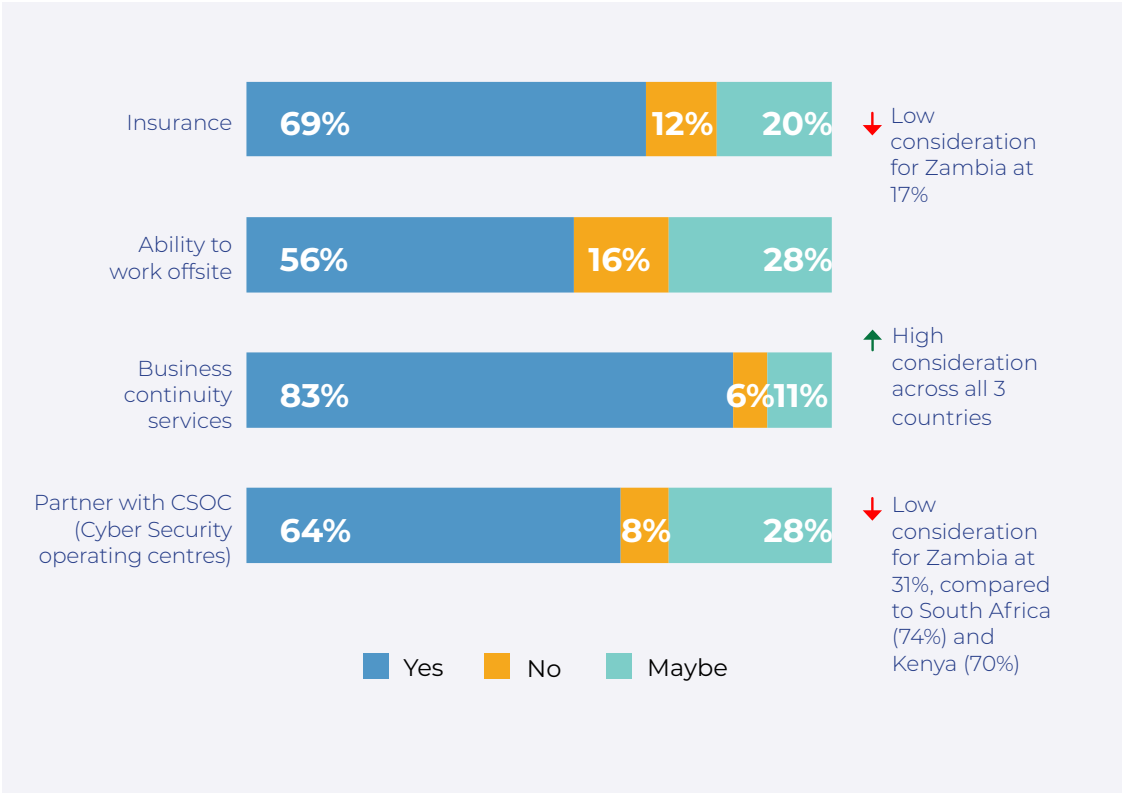
To mitigate the threat, 72% of companies have implemented advanced endpoint protection with data backup (51%) and secure VPN and remote access (44%), coming in at second and third place, respectively. There has also been a marked increase in two-factor authentication, email content filtering, malware detection, and web content filtering since 2021.



Companies are paying attention to the security controls and safeguards they need to put in place to mitigate the threats, but there needs to be more of a focus on data protection. Solutions such as web application firewalls and penetration testing should become more of a focus alongside endpoint detection and response in the form of managed detection and response that ensures constant event monitoring and visibility into the security environment.

It has become critical that organisations have the tools and platforms to rapidly identify and address these threats and engage with managed security services providers that can shift their security approach from a reactive stance to a proactive one. This is a need that organisations have identified, with 64% prioritising partnering with a cyber security operating centre and investing in cyber security services that enable their ability to work offsite (56%).

.

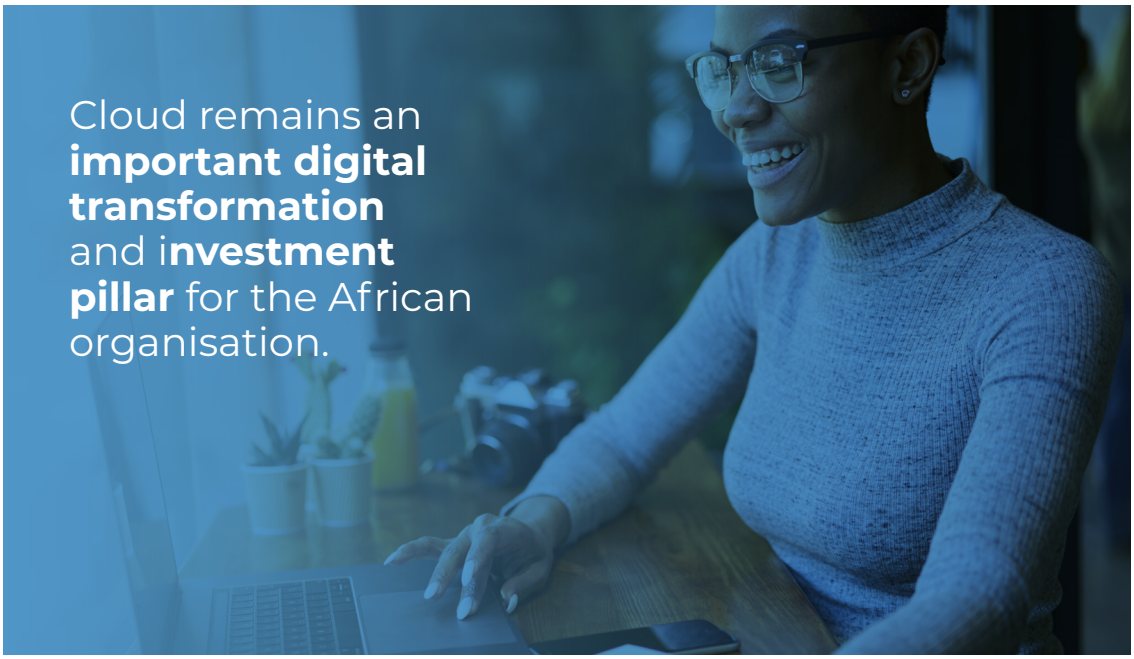


Securing the cloud

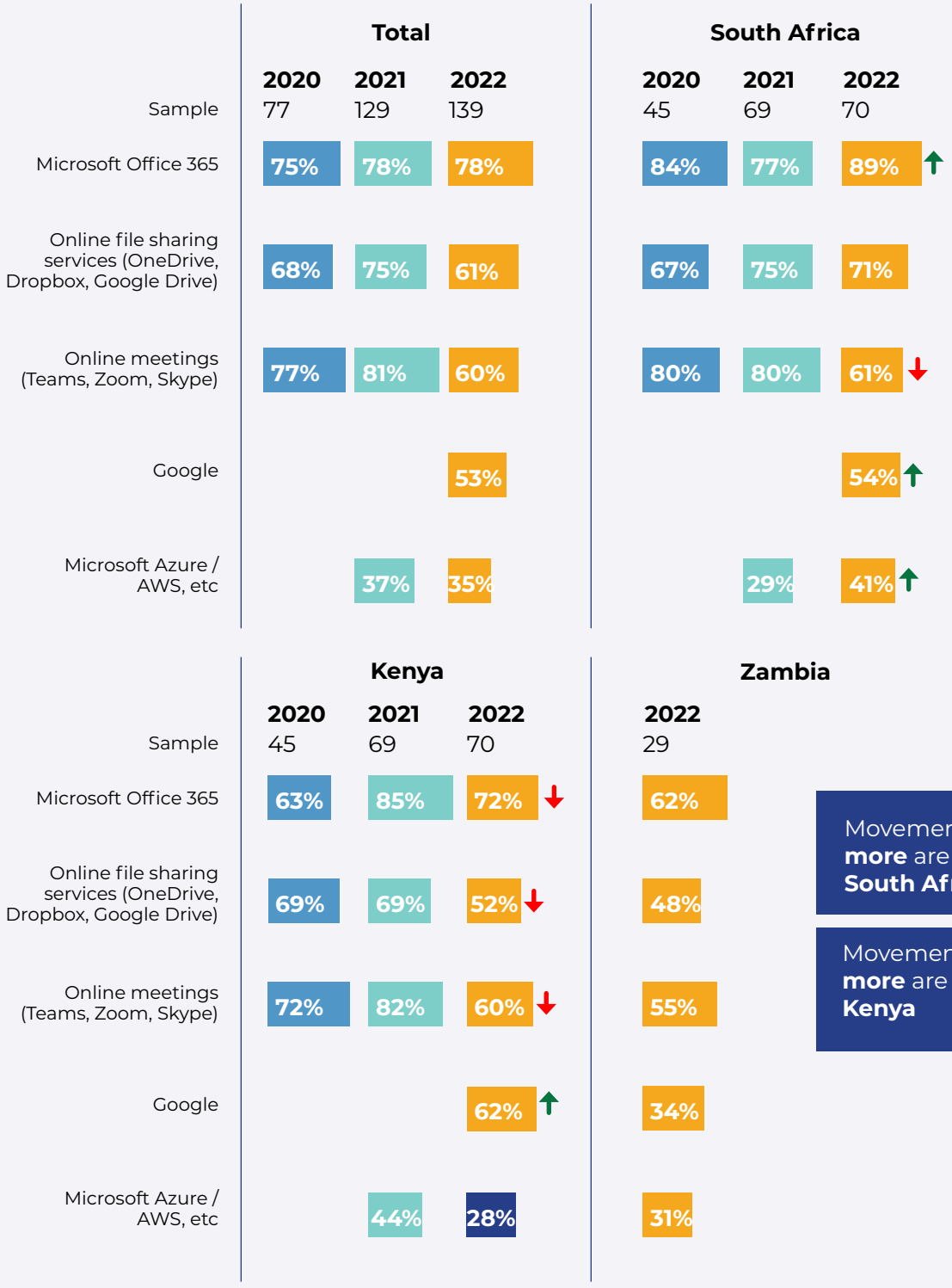
Cloud remains an important digital transformation and investment pillar for the African organisation. It is also linked to some of the most prevalent types of

cybercrime currently affecting these organisations and their perceptions of these crimes. For example, email is linked to how people work and their use of cloud-based platforms, while companies in South Africa are more concerned with data breaches, those in Kenya are primarily worried about managing user access to information.

Microsoft remains the most popular cloud-based service in use by organisations in Africa at 78% - an increase on 2020 (75%) but the same as in 2021 (78%). However, Google has seen a significant increase at 53%, and online file-sharing platforms such as Google Drive, OneDrive and Dropbox have dropped from 75% in 2021 to 61% in 2022. Google is used primarily by small to medium-sized companies in South Africa but across all sized companies, including enterprises, in Kenya and Zambia.



Type of cloud-based services being used



Movements of **8% or more** are noted for **South Africa**

Movements of **12% or more** are noted for **Kenya**

Overall, 65% of companies have a digital adoption strategy or roadmap, with South Africa in the lead at 70%, followed by Kenya (68%) and Zambia (52%), showing that there is a clear sense of purpose when it comes to planning cloud investment for the future.

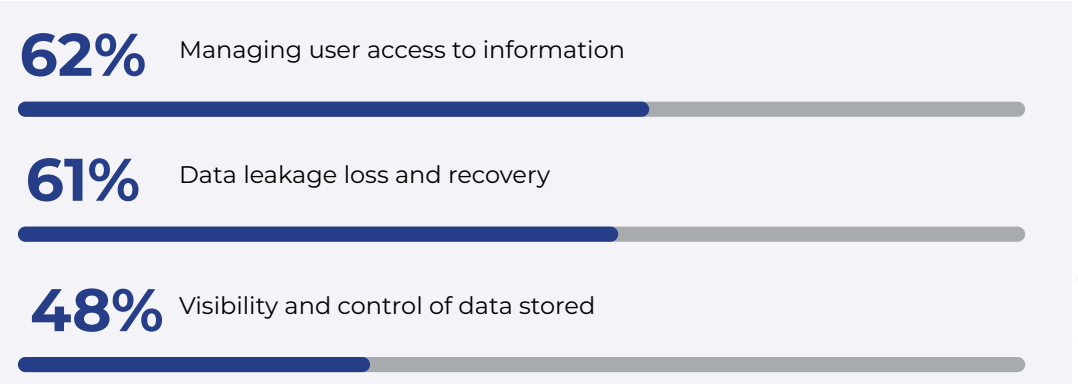
The key elements of cloud adoption strategy across all three countries are primarily focused on security (60%), with this percentage broken down into data security (29%), hacking (4%) and network security (2%). The remaining 50% was balanced across strategic cloud investment for business (14%) and cloud services (22%). The latter saw most countries looking to develop a universal cloud system (9%), optimise cloud (5%) and migrate to a new cloud solution (3%).

However, the concern is that the average spend on staff training is low at 15%, which indicates that there is not enough emphasis on the behavioural and people element of cyber security. According to respondents, staff training is the investment that delivers the least return on investment (ROI) at only 4% – a concern in light of how people are most often the weakest link in any security strategy.

Some of the key elements that companies perceived to deliver the most ROI were:

As highlighted above, the concerns that dominate cloud-based services are primarily managing user access to information, data leakage loss and recovery, and visibility and control of data. These concerns align with the changing world of work and the growing reliance on cloud-based services and solutions.

The top three security concerns around cloud-based services were:

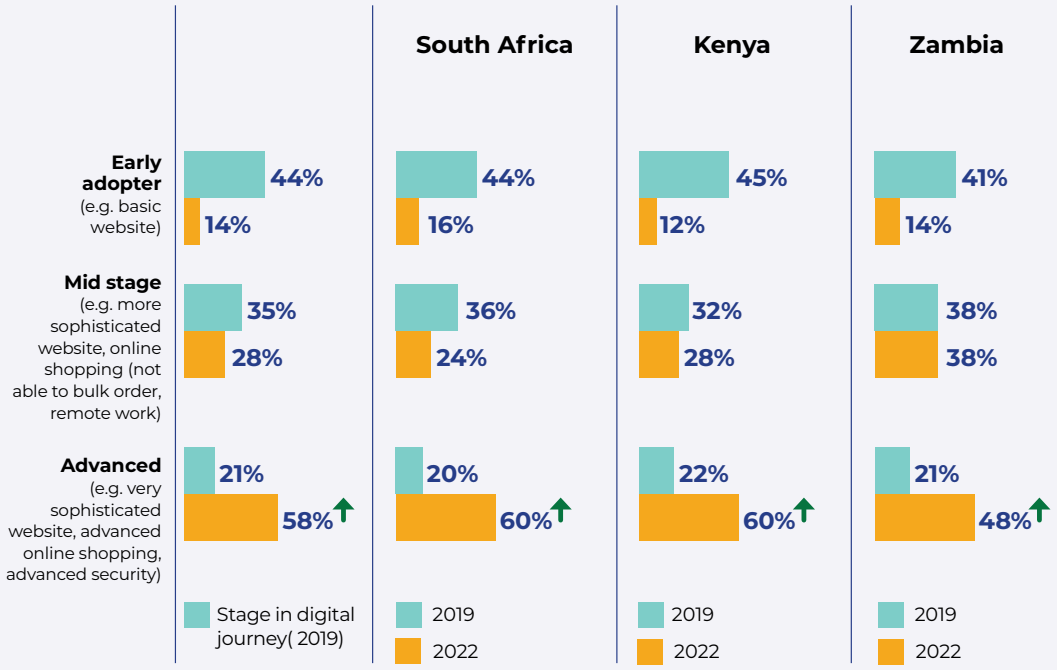


The Sophistication Equation

While several key trends emerged within this report and over the past three years, the golden thread that runs through 2022 and into 2023 is the perception of sophistication. All respondents highlighted that they had advanced significantly in their cloud and digital strategies and cyber security capabilities. In 2022, 58% of companies felt that their digital platforms and strategies were sophisticated with

advanced security and services, compared with 21% in 2019. In fact, most were in the early stages in 2019 (44%) compared with only 14% today, and this has led most to believe that they are more sophisticated and have more protection.

Companies were asked what best described their digital journey in 2019, and what best describes their digital journey now in 2022.



Companies believe they are making significant progress in their adoption of strategies to combat cyber threats

While it is true that companies are making significant progress in adopting strategies to combat cyber security threats, it is crucial for them to acknowledge that criminals are even more sophisticated. Therefore, it is essential that organisations continue to invest in cyber security strategies, systems and methodologies that allow them to stay ahead of the complex threat landscape and mitigate the ever-evolving risks.

Cyber security investment

The current landscape is complex. Organisations are facing tight economic conditions with a rising cost of living, economic volatility, socio-political complexity, and ongoing limitations around talent and resources. The latter is a key issue – the continent lacks the talent and resources required to deal with cyber security threats. According to the Africa Center for Strategic Studies, the continent faces a growing 100,000-person gap in certified cyber security professionals. However, this number may disguise the true magnitude of the problem as there is no readily available data on the level of investment made by African governments into cyber security.

> "Africa is a continent of approximately **1.24 billion people**, yet it is estimated that there are only **7,000 certified security professionals** or one for every 177,000 people."
>
> Assessing Cyber security Policy Effectiveness in Africa via a Cyber security Liability Index.

With this picture in mind, the report examined how organisations invest in their cyber security personnel and systems. When asked if they had appointed cyber security staff members or signed up with a cyber security team in the past year, 68% said yes, and 32% said no. Kenya had the highest yes percentage at 82%, followed by South Africa (63%) and Zambia (62%).

Of the 32% who said no, the top reasons behind this decision were:

20% Financial difficulties and constraints prevent them from doing so. This was the highest in South Africa.
and;
Already outsourcing.

14% Already have well-equipped systems.
and;
Have said it has not been necessary.

9% Have an internal skillset.

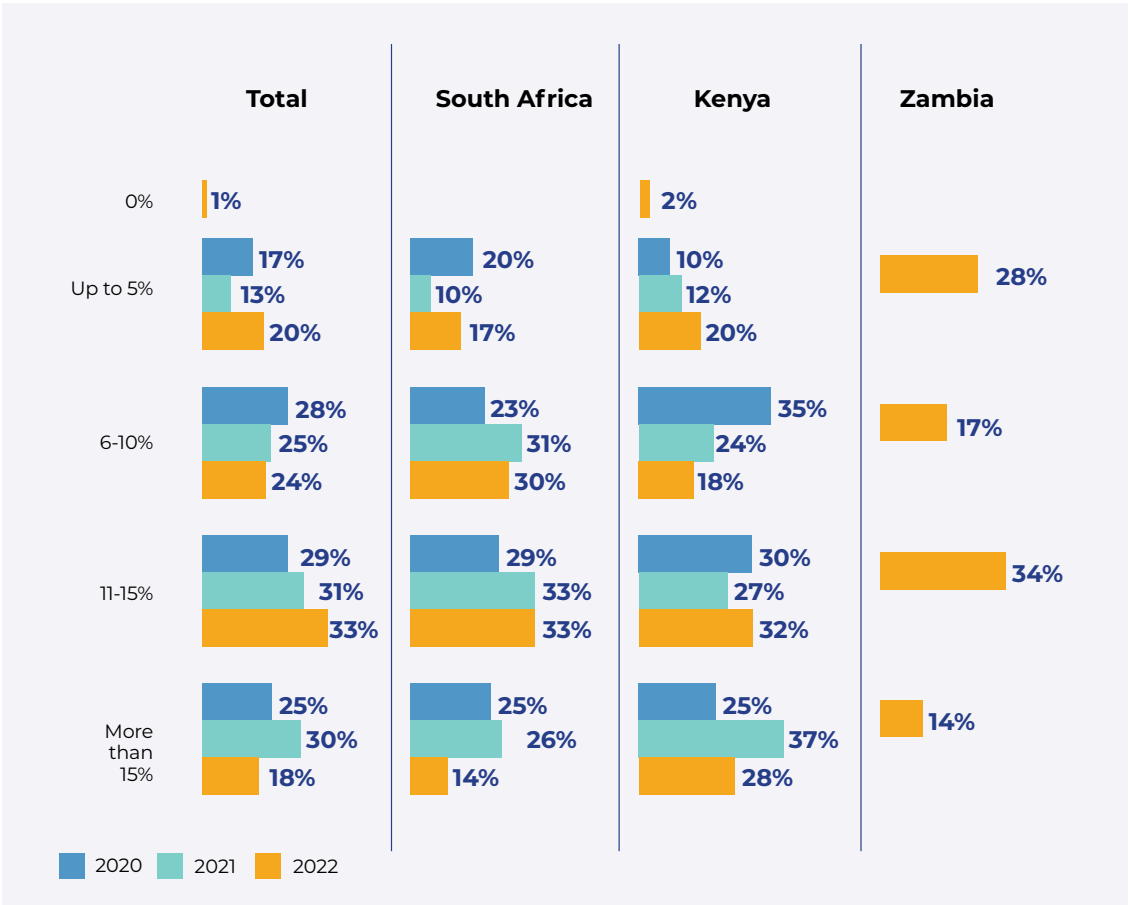
7% Adequate staff.

The concern for countries like South Africa, where financial strain limits cyber security investment, is that they are under intense pressure to perform to ever-higher security expectations with increasingly lower budgets and limited expertise when accompanied by the growing talent shortage.

The percentage of the IT budget allocated to cyber security saw significant shifts over the past three years. In 2020, companies that had allocated more than 15% of their IT budget to managing cyber security sat at 25%. This increased to 30% in

2021 and then dropped to 18% in 2022. In the category of companies that dedicate 11-15% of their IT budget to cyber security, the investments have remained relatively the same from 2020 (29%), 2021 (31%) and 2022 (33%). Across all three countries, this is the most common range of IT spend towards security, with the remainder split fairly evenly across the 6-10% and 15% ranges.

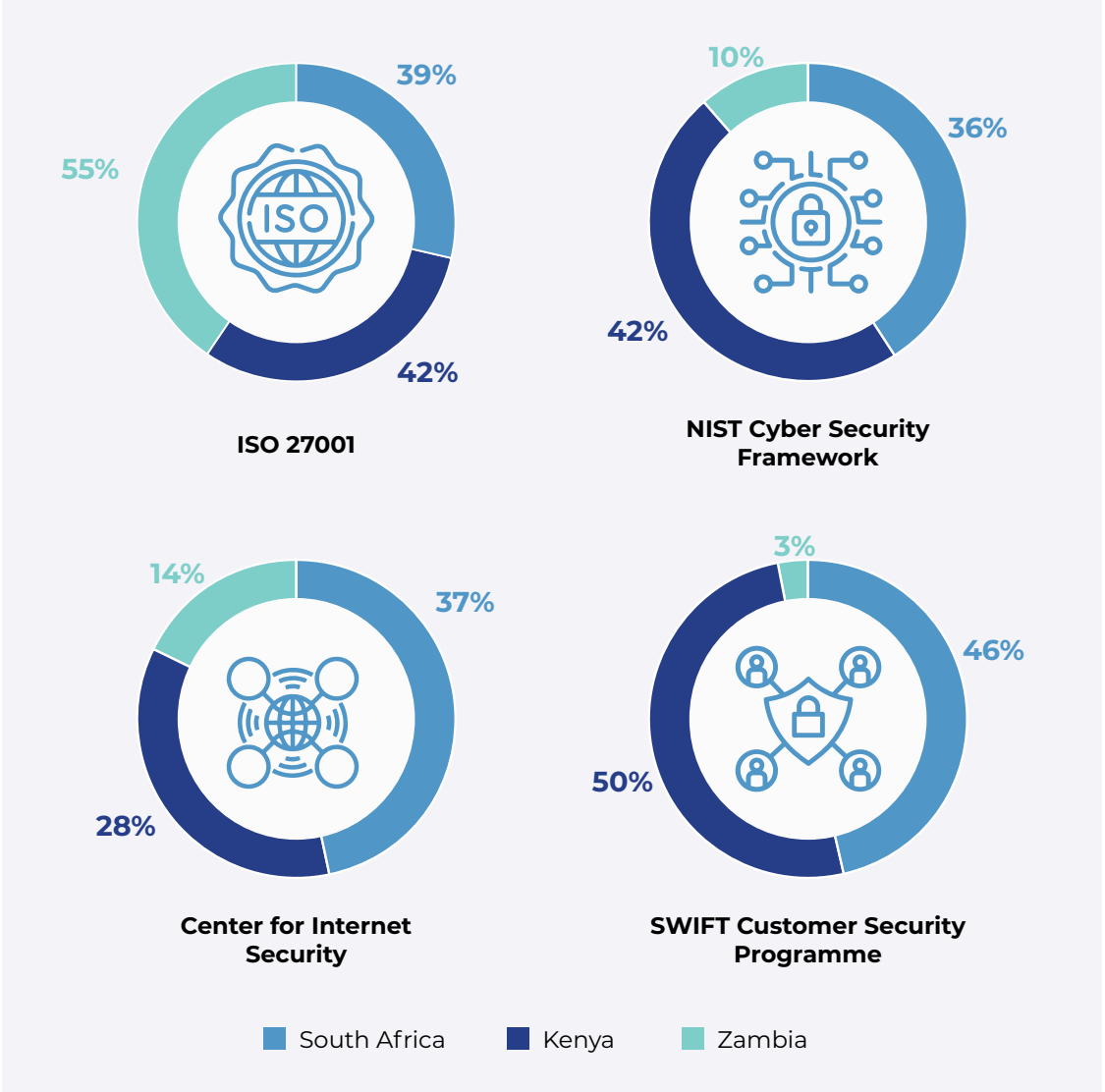
The minimum spend should sit at 15%, possibly even up to 20%, in light of how severe the threat landscape is right now and how costly the fall-out is in the event of a successful attack.



When it comes to the claimed budget spent per employee on managing cyber security, the average spend in South Africa in 2022 was more than R250 per employee per month – a significant increase of 31% over 19% in 2021 and 10% in 2020. In Kenya, the large banking and finance, communication, agriculture and manufacturing sectors showed a measurable increase in this spend of 20% in 2022 compared with 10% in 2021, averaging at $50 or more per employee per month.

Zambia, however, had 48% of companies respond with 'don't know' and only 14% with $15-$50 per employee per month.

The respondents cited their use of the following industry frameworks:



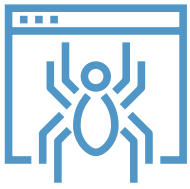
In conclusion

There has been a significant decrease in inadequate safety, security and protection of data in 2022, with a majority of organisations moving much further down the digital adoption road. There is a marked increase in awareness and the implementation of cyber security measures post the global pandemic. However, nearly two in three companies experienced a data breach in the past year, and the most significant threat remains hacking across all three countries, even more in Kenya. This is closely followed by unauthorised access and cyber-attacks, with companies concerned about confidential information being stolen or accessed, particularly in Kenya and Zambia.

South African and Kenyan companies are still worried about the financial and reputational impact of an attack, while Zambia is primarily concerned with the disruption to the business. As hybrid working continues to gain traction and adoption, the biggest threats to the business are seen as coming through email, making it imperative that companies focus on protection and security in the hybrid environment. Given the limited attention paid to training and education, this is one of the critical factors that companies should be paying attention to moving forward, along with password protection on laptops and regular reminders to staff members.

Cyber security teams are in place at around two-thirds of companies, but there remain challenges around costs, particularly in South Africa. Approximately 7% of companies say they outsource to ensure they have the necessary skills, but the cost and allocated budget are issues. This is reflected in how the budget for cyber security as a percentage of IT spending hasn't changed since 2021.

The Zambian market appears not as advanced as South Africa and Kenya, which could be either a result of low awareness or fewer threats. On the other hand, Kenya appears to be the most aware, as 90% of respondents had a data breach in the past year.



*As hybrid working continues to gain traction and adoption, the **biggest threats to the business** are seen as coming through **email,** making it imperative that companies **focus on protection and security** in the hybrid environment.*

South Africa

Companies in the region cite hacking and gaining unauthorised access to information systems and assets as the biggest threats, with the financial impact of a breach the most serious concern. South Africa favours the hybrid model of working with in-office employees, only having seen a 3% increase from 2021.

Kenya

Kenyan respondents feel illegal access to information is a great concern and perceive the single biggest impact to be damage to reputation and the company's credibility in the event of a breach. Kenyan companies seem to be migrating back to 100% in-office work, with an increase from 34% in 2021 to 50% in 2022. This is perhaps influenced by the fact that Kenya has seen a rise in data breaches, with four in five respondents having experienced one in the past year. Some Kenyan companies have traded Microsoft Office 365 (down 13% year-on-year) for Google, which is now 62%.

Zambia

Companies in the region cite data loss, including data exfiltration or leakage, as a concern and put business disruption as their most considerable perceived fall- out at 31%, which is higher in comparison to the 12% average across all countries.

Although Zambia recorded the lowest threats compared to other countries, 62% say the threats have increased in the past year. Interestingly, Zambia does not support a solely remote working model, with 55% being in the office and 45% following a hybrid model.

The Liquid C2 perspective

Cyber security attacks are more virulent, sophisticated and frequent today than ever before. This makes it even more challenging for companies to defend against them and makes it critical for cyber security to remain at the heart of every business conversation. The report revealed a landscape where companies prioritise security but remain constrained by limited access to talent and budgets. This is why it has become vital for organisations to collaborate with trusted third-party managed security services providers (MSSPs) to reinforce and refine their security postures while remaining aligned with budgets and spend.

"Perhaps the biggest concern emerging from this report is that companies are saying that they've put **a lot more cyber security controls in place."**

Meaning they are not as concerned because the threats are evolving at a faster rate than security systems, and companies cannot afford to get complacent."

Essential areas of focus

Endpoint detection and managed services

Companies should invest in solutions such as endpoint detection and response (EDR) or leverage EDR services provided by a reliable MSSP to help minimise and mitigate hacking and malware threats. Liquid offers MDR services 24/7/365, ensuring companies have rigorous visibility into their environments and what's happening within them. We provide organisations with the transparency they need to remain in control of their security while rapidly identifying possible threats and addressing them at speed. With our services, organisations shift from a reactive stance to a proactive one – making decisions based on situational awareness and leveraging tools such as penetration testing to consistently catch and address vulnerabilities and areas of weakness.

The protection of data

There is far too little focus on the protection of data across all companies, with limited visibility into who has access to the data, the location of the data, those accessing it, and the protection of this data across multiple devices and platforms. There are ongoing concerns around the physical theft of laptops, whether the data is encrypted or adequately stored, and who now has access to privileged corporate information. This makes it essential to implement controls that empower companies to fully realise the potential of their cloud investments and hybrid working environments.

Leveraging the Liquid C2 MSSP bouquet of services, companies gain access to solutions that allow for robust digital rights management, encryption tools, and tokenisation tools to be implemented intelligently throughout the ecosystem. Key in terms of data is access control, and so we ensure that systems, applications and databases have native capabilities enabled and that the proper access controls are put in place. This includes identity and access management, data situational awareness, and how the data is shared, managed and stored.

Email remains a priority

Email is still a concern, and it should be. The first line of defence should be email protection – nobody should receive an email until it has gone through the proper filtering and checks to mitigate the risks of phishing, spam and malware, among others. Regardless of the organisation, email should flow through rigorous checks and balances before it reaches the end user. Liquid can C2 it that your business has all the right measures in place – ensuring that you have multi-layer protection and robust threat controls to ensure that email remains an asset, not a risk.

As ransomware, a threat that still uses email as one of its primary distribution mechanisms remains a high threat, Liquid offers Bullwall RansomCare – a solution that picks up when the ransomware encryption is initiated and stops it from continuing. This limits the impact of the ransomware attack and significantly reduces the threat and any potential damage.

Cyber security investment

Cyber security should be high on the agenda of the organisation. The risks are evolving, and their sophistication is increasing. This is further complicated by the rise of compliance across legislative and regulatory requirements worldwide. In addition, organisations need to pay attention to user awareness and training to mitigate the serious risk of user error – no matter how sophisticated the system or advanced the controls, human error is a huge contributing factor to security breaches.

Security awareness campaigns are essential, as is skills development. Liquid provides organisations with phishing simulations as part of a cohesive cyber security awareness campaign that allows for ongoing training and awareness.

Another area that requires a change is the levels of cyber security investment. The survey found that the majority of companies have their investment sitting in the 11-15% bracket, but the reality is that they should be spending at least 20% on average to ensure that their cyber security posture is robust enough to handle the threats. It is a concern – companies need to find a balance between their IT spend for growth and their cyber security spend for protection. Liquid can provide organisations with customised security management and controls that blend seamlessly with cloud investment strategies and remote or hybrid working frameworks.

Our skillsets and broad range of expertise ensure that any skills gaps within the organisation are easily overcome. We provide the tools and services required to deftly manage cloud systems, data protection, email, and more. Our capabilities across Microsoft, Google and multiple other cloud platforms mean that you don't need to invest into in-house talent, as we can help you integrate and secure your digital investments with ease.

Security by intent and design

Liquid aligns with security by design principles to ensure the development of a resilient and relevant cyber security framework. We help you to build 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 defences in-depth, and implementing fail securely, among many other capabilities.

We collaborate with intent - we know that there are multiple factors to consider and that each business is unique. So we create a cyber security framework and posture that delivers reliable protection against cyber security threats, cyber-attacks, data loss, data breaches and more.

Find out how Liquid can deliver cyber security that meets your expectations and your needs here:

www.LiquidC2.com

LinkedIn 

Facebook 

Twitter 

Email