ARCTIC WOLF

REPORT

The State of Cybersecurity in South Africa 2023

In today's rapidly transforming world, every enterprise with a digital footprint, regardless of its sector or the nature of its business, is vulnerable to cyber attacks and breaches.

TABLE OF CONTENTS

FOREWORD

As the market leader in security operations, Arctic Wolf understands the critical importance of staying ahead of the evolving threat landscape. Over the past few years in particular, we have witnessed an alarming upsurge in cyber attacks targeting businesses of all sizes in South Africa.

From phishing scams to ransomware attacks, cybercriminals are using increasingly sophisticated techniques to steal sensitive data and cause financial harm to their victims. As a result, it has become essential for businesses in South Africa to take a strong, proactive approach to cybersecurity.

The 'State of Cybersecurity in South Africa 2023' report was compiled based on the results of a South African survey conducted in February 2023, in partnership with ITWeb, amongst 163 South African IT and security professionals.

This survey was commissioned by Arctic Wolf in order to gain a clearer understanding of the South African market, ascertain where local businesses are on their security transformation journeys, and what their biggest challenges are.

Research Methodology

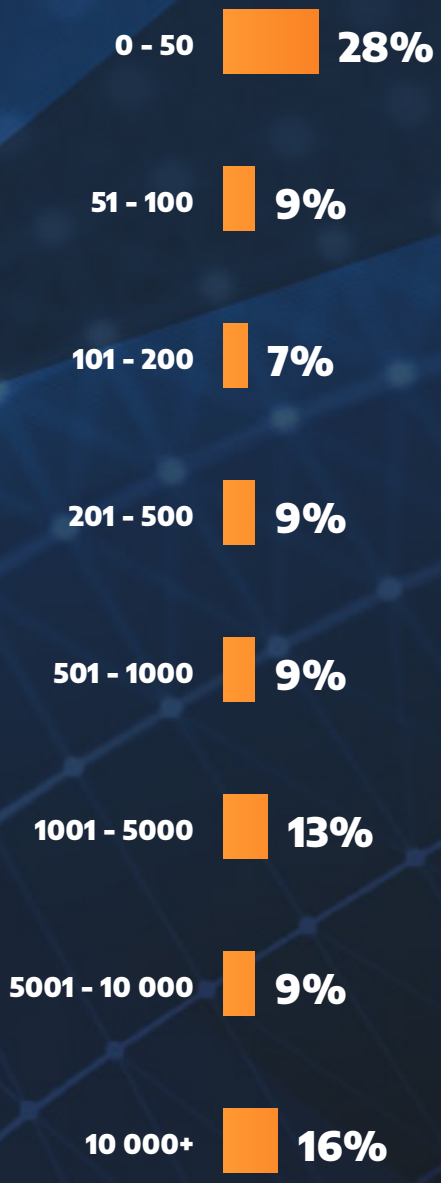
The intention of the Arctic Wolf State of Cybersecurity in South Africa 2023 survey was to identify the most significant threats and vulnerabilities facing local businesses today, and the main areas of business concern for 2023, as well as to gauge local opinion on whether organisations should be legally required to disclose a cybersecurity incident or data breach.

Almost 70% of respondents to the survey (68%) were from middle management positions, with 41% representing C-level management, and 38% IT staff (all other non-management positions). Consultants represented 21% of the survey, and 8% held 'other' capacities.

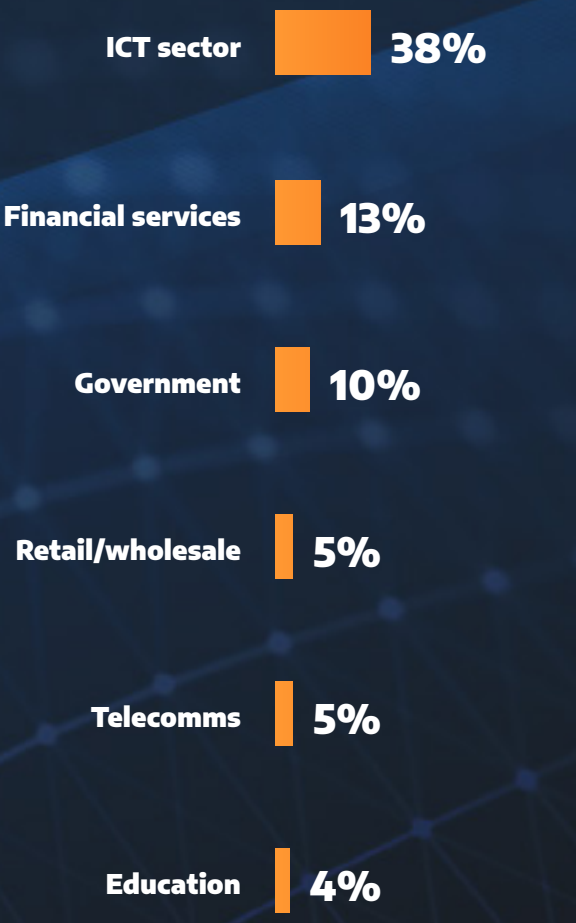
With regards to reporting structure: 31% percent of those surveyed did not have any staff reporting directly to them; 44% had fewer than 10; 16% had between 10 and 49; 5% from 50 to 99; 1% from 100 to 199; 1% between 500 and 999; and 2% had more than 1,000 employees reporting to them.

 | |

Company Size



Industry



Non-ICT-related professional and business services, media, manufacturing, healthcare and pharmaceuticals, automotive, tourism, hospitality and leisure, parastatals and utilities. **2%**

Transport, non-government and non-profit entities, construction and engineering, advertising and marketing, mining and petrochemical, and consumer goods and services. **1%**

Executive Summary

Arctic Wolf's survey has identified several challenges businesses in South Africa have faced in their security transformation journeys over the past year, and shows that the top concern for 2023 is ongoing cyber attacks.

Other areas of continued apprehension included a shortage of skilled personnel, where an evolving, expanding threat landscape is giving rise to increasing, more sophisticated cyber attacks, which in turn require more skilled resources. The 'Great Resignation', which saw record numbers of individuals leave their jobs over 2021, has also had a negative impact on qualified skills availability, as has the increasing opportunity for remote work, which has opened up the doors for foreign recruitment of local talent.

Furthermore, inflation - and its impact on cybersecurity budgets - was another key concern for 2023.

Despite these challenges, the survey revealed that organisations in South Africa are taking positive steps to improve their security posture, with the majority of local businesses increasing – or at the very least maintaining - their cybersecurity budgets over the next 12 months, denoting that cyber attacks remain a key concern for management's agendas in the new year.

The security strategy is maturing in South Africa. 24x7 eyes-on service is becoming extremely important to build business resilience for organisations. In line with this, almost two thirds of the businesses in question (64%) indicated that they would consider implementing a 24x7 security operations service moving forward.

Overall, the survey highlights the need for organisations in South Africa to prioritise their security transformation journey and address the challenges they face. It underscores the fact that businesses should be partnering with organisations that deliver 24x7 security operations, while providing proactive security, threat and vulnerability management. By allowing the experts to step in and keep the organisation secure, companies are then freed up to focus on their own core services.

Jason Oehley
Regional Sales Manager,
Arctic Wolf

 | |

Key Findings

The survey revealed the following key findings:

01

Nearly three quarters (74%) of the survey respondents said that their cybersecurity budget for 2023 would increase, with 22% stating that it would remain the same.

02

The top three areas of concern for businesses going into 2023 were continued cyber attacks (77%), the talent shortage (47%), and inflation (38%).

03

The types of cyber attacks that businesses are most concerned about facing this year were as follows: ransomware (77%), business email compromise (62%), and cloud breach (46%).

04

In the past 12 months, three quarters of participants (74%) have received an email at work that they believe to be a phishing attempt to collect their credentials. Almost half (47%) have received an email or text message that they maintain impersonated an executive at their company. Another 47% have received an invitation or message on a social networking site (LinkedIn for instance) that they believe to be malicious in nature.

05

Security incidents experienced over the past 12 months include: business email compromise (37%), ransomware (18%), disinformation campaign (17%), insider threat (15%), cloud breach (12%), and supply chain attack (12%).

06

The majority of respondents (85%) says that businesses should be legally obliged to disclose a cybersecurity incident or data breach.

07

A third (33%) of those surveyed said their organisations had experienced a cyber incident in the past year. Half of respondents (52%) said that they had not.

08

Of those who replied 'yes' to the question above, 57% had experienced a business email compromise (BEC), 14% a ransomware attack, 14% a cloud breach, and 14% an insider threat.

09

While 72% of the survey participants may have 24x7 security tools running, far fewer are actually constantly monitoring their security profile and tools. The goal should be for businesses to have eyes-on security around the clock.

Types of Threats Experienced in 2022

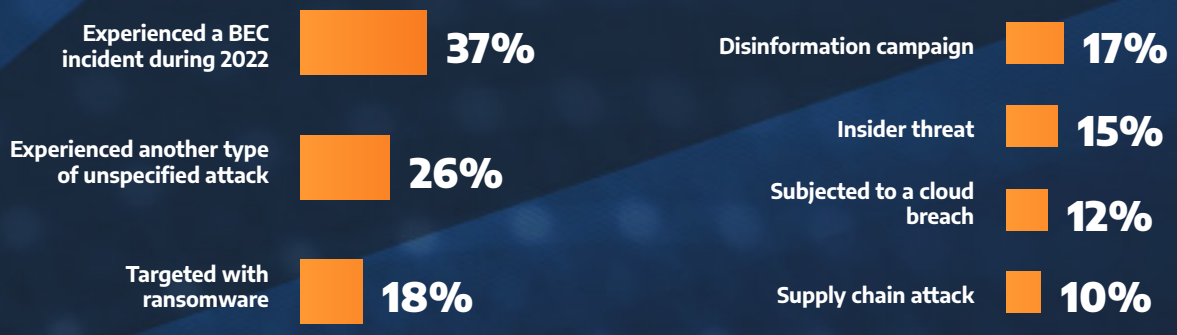
High-profile cases continued into 2022, with local organisations including high profile customers across verticals being targeted in cyber attacks.

For the past few years South Africans – both businesses and individuals - have been under siege as never before from a cybersecurity perspective.

In 2020, Accenture[1] reported that South Africa had the third most cybercrime victims worldwide, losing R2.2 billion a year, with low investment in cybersecurity and immature cybercrime legislation making the country a serious target.

These statistics were further supported by INTERPOL's African Cyberthreat Assessment Report 2021[2], which revealed more worrying local figures, including the fact that South Africa had seen 230 million threat detections in total between January 2020 and February 2021, with 219 million of these detections related to email threats. South Africa also had the highest targeted ransomware and BEC attempts, and the country had also seen a 100% increase in mobile banking application fraud and was experiencing increasing numbers of cryptocurrency scams.

The results of our recent survey are aligned with these figures, as businesses responding advising that:



[1] https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa
[2] https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa

 | | Public

With regards to suspected malicious messaging attempts:

Received an email that they believed to be a phishing attempt to collect credentials	75%
Received a message on a social networking site that they believed to be malicious in nature	47%
Received an email or text impersonating an executive within their business	47%
Received none of these types of messages	13%

Overall, 33% of participants had been exposed to a security incident over the past 12 months. While 52% advised that they had not, and 15% were unsure, these figures could potentially be attributed to the fact that discussing security breaches is a difficult subject. In Arctic Wolf's experience, not all organisations approached will provide information on the actual security breaches to which they have been subjected, but we have found that the majority have seen a drastic increase in attempted attacks at the very least.

Concerns for 2023

REAL APPREHENSION AROUND CONTINUED CYBER ATTACKS

CYBERSECURITY SKILLS SHORTAGE

INFLATION RATES

PHYSICAL SUPPLY CHAIN DISRUPTIONS

CYBER RISKS AND ELEVATED GEOPOLITICAL CONFLICTS

STOCK MARKET VOLATILITY

Top Challenges for 2023

Factors that have contributed to changes within the cybersecurity landscape include a continued focus on remote working, increasing use of artificial intelligence (AI) and machine learning (ML) tools, more emphasis on cloud-based systems, and growing numbers of Internet of Things (IoT) devices in use.

This constantly evolving environment has given rise to an increased need for stringent security measures, and our respondents agree, advising that their top concerns for 2023 include real apprehension around continued cyber attacks, with almost three-quarters (74%) placing this at the top of the list of concerns.

The shortage of cybersecurity skills was listed as the next greatest concern, with 53% of those surveyed making note of the talent shortage. This fear is not unfounded, as noted in the Information Systems Audit and Controls Association's (ISACA) State of Cyber Security 2022 report[3], which observes that key threats to the shortage of cyber resources are talent poaching, insufficient financial incentives, and limitations to career growth and development. The study also stated that after the 'Great Resignation' trend of 2021, employees are demanding increased work flexibility and higher wages.

Inflation was documented as a close third area of concern (52%) by our survey participants. Increasing inflation rates can have a profound, multilayer effect on cybersecurity. Price increases can lead to serious budgetary concerns for businesses, from growing staff wage costs to more expensive technology products and services, meaning that they may need to reconsider where their spend is going. Cybercriminals too are not exempt from the pressures of rising inflation rates, leading to an increased number of cyber incidents which are also more costly in nature.

Cybersecurity plays a critical role in protecting the physical supply chain, which involves the movement of goods and material from suppliers to manufacturers, distributors, retailers, and ultimately to consumers. The supply chain is becoming increasingly reliant on technology and digital systems, which also makes them more vulnerable to cyber attacks that can disrupt operations and compromise sensitive data. This is clearly top of mind for our research participants, with 30% listing physical supply chain disruptions as another area of concern for 2023.

The combination of cyber risks and elevated geopolitical conflicts ranks high on the list of global threats that could negatively affect businesses worldwide, according to PwC's 25th Annual Global CEO Survey, January 2022[4]. Geopolitics will continue to influence cybersecurity and organisations' security postures into 2023 and beyond, and was of concern to 23% of our survey respondents.

Finally, our results showed that stock market volatility was mentioned by 9% of those surveyed, with cyber attacks able to negatively impact stock prices.

[3] https://www.isaca.org/go/state-of-cybersecurity-2022
[4] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cybersecurity-geopolitical-conflict-board-ceo-response.html

Greatest Cyber Attack Apprehensions for 2023

When it comes to ransomware. South Africa is one of the most targeted countries, not only on the continent but also in the world, so it stands to reason that more than three quarters (77%) of our research respondents listed this as their top cyber attack worry for 2023.

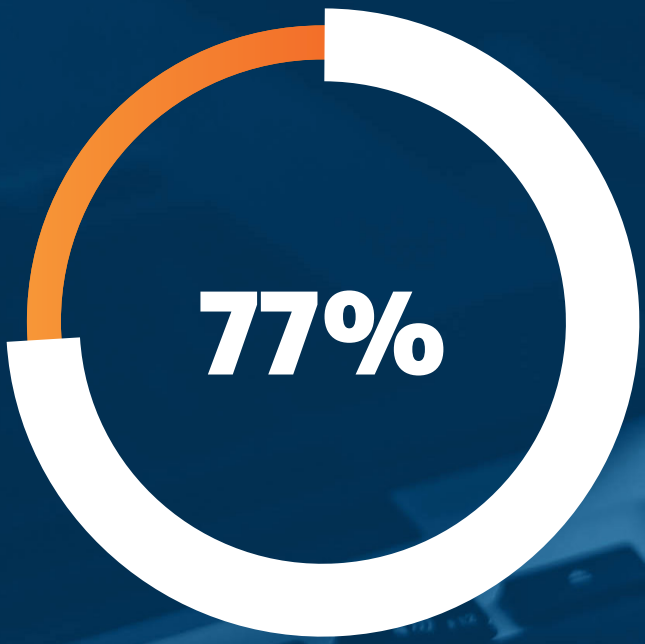
This was followed by BEC incidents at 62%, an area of legitimate concern due to continued remote working environments. Growing local cloud adoption is also indicated in our responses, with 46% of businesses listing cloud breaches as an area of great concern for this year.

Insider threats, which are also exponentially on the rise and can be malicious or unintentional acts of negligence, came in as our fourth highest area of concern, as noted by 34% of respondents.

As noted previously, supply chains can present many vulnerabilities and thus opportunities for cybercriminals to attack, leading to disruptions that can affect many organisations and individuals. Supply chain attacks for this year were a worry for 19% of those contributing to our survey.

Disinformation campaigns, which can be described as false information deliberately spread to deceive people, have become more commonplace across the African continent. As it has also become more difficult to discern legitimate information from 'fake news', 19% of our respondents have listed this as an area of continued emphasis for the year.

 | |



TOP CYBER ATTACK WORRY FOR 2023

RANSOMWARE

Cybersecurity Budgets for 2023

There are several reasons why businesses in South Africa should continue to focus budgetary resources on cybersecurity measures for 2023:

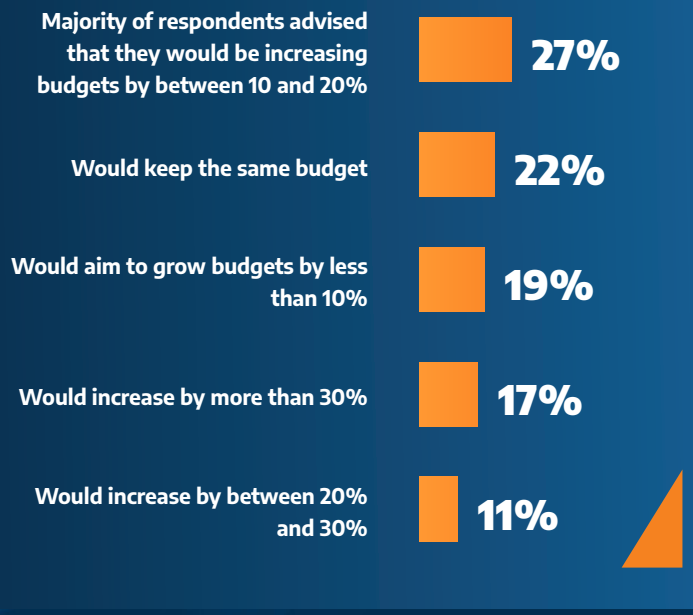
To avoid the significant financial losses and reputational damage that can be attributed to cyber attacks.

To ensure compliance with South Africa's stringent compliance regulations, such as the Protection of Personal Information Act (POPIA) and the Cybercrimes and Cybersecurity Bill.

To protect a growing remote workforce.

 | |

Our report showed heartening results:



Those that plan to decrease cybersecurity budgets would scale down by less than 10% (2%) or by more than 30% (1%)

Disclosing a Cyber Attack or Data Breach

The disclosure of a cyber attack or data breach is important for a number of reasons, such as the importance of transparency and accountability to customers and stakeholders, and the rebuilding of trust.

By disclosing the breach, an affected business is also able to take steps to mitigate the damage caused by the breach, which could include informing those affected and implementing stronger, preventative security measures and collaborating with law enforcement agencies.

Our research showed that 85% of our respondents agreed here, believing that organisations should be legally required to disclose a security breach.

 | |

BELIEVE THAT ORGANISATIONS SHOULD BE LEGALLY REQUIRED TO DISCLOSE A SECURITY BREACH

Conclusion

In today's rapidly transforming world, every enterprise with a digital footprint, regardless of its sector or the nature of its business, is vulnerable to cyber attacks and breaches. And because we are faced with more, increasingly sophisticated threats on a daily basis, it is imperative that South African organisations continue to build their cyber resilience. It is only through a strong cybersecurity posture that we will be able to deal with ongoing threats, challenges and crises, while gaining competitive advantage and protecting reputations.

However, businesses cannot do this alone. By partnering with a cybersecurity operations leader, like Arctic Wolf, organisations are able to establish a non-stop security operations approach. This will ensure the delivery of an effective cybersecurity service, protecting the customer 24x7, as well as the education of its extended staff complement on security-related issues. In turn, allowing an expert partner to deliver security operations and guidance - while integrating with existing security tools – also allows for a reduction in the requirement for internal security skills.

 | |

About Arctic Wolf

Cybersecurity Redefined

In the era of digital transformation, many organisations find it a never-ending struggle to defend against rampant cybercrime. That's why you need the experts in your corner.

Arctic Wolf® is a global leader in security operations, delivering a premier cloud-native security operations platform designed to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyses more than two trillion security events a week across the globe, helping enable critical outcomes for security use cases and optimising customers' disparate security solutions. The Arctic Wolf® Security Operations Cloud delivers automated threat detection and response at scale, and empowers organisations of virtually any size to establish world-class security operations with the push of a button.

END CYBER RISK

ARCTIC WOLF

For more information please visit arcticwolf.com or
contact us arcticwolf.com/uk/company/contact-us/