SYBERKONSULT

2024 Cybersecurity Report

Welcome to the 2024 Cybersecurity Report by SyberKonsult. We are excited to share this comprehensive document with you, which covers a wide range of topics including recent cybersecurity developments, the current landscape and trends, and our forecasts for the future of cybersecurity. Our team of experts has meticulously analyzed data from various sources to provide you with the most up-to-date insights. This year, we've observed significant advancements in threat detection and prevention technologies, as well as an increase in sophisticated cyber-attacks targeting both large enterprises and small businesses as well as government institutions.

The first section delves into our firm's mission, vision and story. We then cover notable incidents in cybersecurity thus far. From Russian hackers' cyber warfare to vanity breaches, we outline what transpired and the impact of such incidents. These are broken down in a monthly timeline format from January 2024.

The second section provides a detailed analysis of the current cybersecurity landscape and trends noted. We highlight the most prevalent threats, including ransomware, phishing attacks, and the most affected regions globally. We then focus into the South African perspective on cybersecurity, exploring how companies perceive and engage with governance, risk management, and compliance.

Looking ahead, our forecast section offers predictions for the future of cybersecurity. We anticipate an increase in cyber threats as technology continues to evolve, making it imperative for organizations to stay ahead of the curve. We explore emerging trends such as quantum computing, blockchain security, and the integration of cybersecurity with other technologies like IoT and cloud computing.

We hope this report serves as a valuable resource for your organization, helping you to understand the ever-changing cybersecurity landscape and to implement effective strategies to protect your assets. Thank you for choosing SyberKonsult as your trusted partner in navigating the complexities of cybersecurity. Stay safe and secure!

Ayabonga L. Jumba
Founder & CEO at SyberKonsult (Pty) Ltd.

What's Inside

Who We Are

SyberKonsult is a professional services firm that provides expertise, guidance, and support in designing, implementing, and managing cybersecurity solutions tailored to the specific needs of the client.

Our key focus is the in-depth protection of IT assets and enhancing the overall security of our client's infrastructure, ensuring sound risk management, compliance and good governance. With a team of highly skilled professionals, SyberKonsult delivers cutting-edge solutions and stays ahead of emerging threats to safeguard your digital environment. We understand that every organization faces unique challenges, which is why we offer customized strategies that align with your business objectives and current growth stage.

Our services encompass a wide range of cybersecurity aspects, including risk assessment, vulnerability management, incident response, and continuous monitoring. By leveraging the latest technologies and best practices, we help you build a robust defence against cyber attacks, ensuring resilience and integrity of your critical systems.

At SyberKonsult, we believe that cybersecurity is not just about technology, but also about people and processes. Therefore, we provide comprehensive training programs to empower your staff with the knowledge and skills needed to recognize and mitigate potential threats. Our goal is to foster a culture of security awareness that permeates every level of your organization.

Partner with SyberKonsult and gain the confidence that comes from knowing your digital assets are protected by experts dedicated to your success. Together, we can navigate the complex landscape of cybersecurity and secure a safer future for your business.

Our Mission

Our mission is to foster and deliver unparalleled digital transformation and security assurance.

At SyberKonsult, our mission is to empower organizations to navigate the complexities of the digital landscape by delivering cutting-edge cybersecurity solutions. We are committed to ensuring the security and resilience of our client's assets in the face of rapid technological advancements, providing expert guidance and proactive risk management to safeguard their future.

SyberKonsult was founded to fulfil the need for state-of-the-art cybersecurity solutions in response to the rapid emergence of new technologies across industries. We operate as a propriety limited company with an R&D partnership with Invidum Technologies for cybersecurity products. Our team consists of Cybersecurity architects, IT Risk specialists and IT Security experts who deliver the best risk management and security implementations, respectively. With our team's wealth of experience, we safeguard our core values and hold ourselves to the highest degree of service. Our founding year of 2024 marks an extraordinary posture of the cybersecurity realm. As a newly minted start-up firm, we have focused on building a robust brand to cement the firm's position in the market. Our mission and vision statement is a testament to our commitment to new-gen solutions for security.

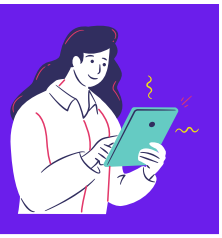
Our Vision

To become the trusted leader in cybersecurity, enabling organizations to thrive securely amidst rapid technological evolution.

To be the leading cybersecurity consultation and advisory firm that anticipates and addresses emerging threats, ensuring security assurance in an era of unprecedented technological change. We envision a future where organizations can confidently innovate and grow, knowing that their digital environments are protected by SyberKonsult's unwavering commitment to excellence in cybersecurity. By fostering a culture of continuous improvement and staying ahead of the curve in cybersecurity developments, we aim to build lasting partnerships with our clients.

At SyberKonsult, we believe that trust is the cornerstone of all successful relationships, and we strive to earn and maintain that trust through our dedication to **integrity, transparency, and innovation**. Together, we will create a safer digital world, where technology serves as a powerful ally in achieving your organizational goals.

Notable Cyber Events



On January 12, 2024, Microsoft detected a cyber attack. The hackers utilized a sophisticated phishing campaign to obtain access to employee credentials, enabling them to breach Microsoft's extensive network. Sensitive data, such as source code, internal emails, and customer information, was compromised. Threat Actor: Midnight Blizzard	January 2024

February 2024	Change Healthcare disclosed on February 21, 2024, that it experienced a cyber attack resulting in the extraction of 4 terabytes of patient data, comprising personal information, payment records, and insurance details. The impact of the attack was substantial, leading Change Healthcare to temporarily shut down certain operations. Threat Actor: ALPHV/BlackCat Cost: According to United Health Group, the attack on Change Healthcare cost them $872 million in the first quarter of 2024.

In March 2024, AT&T faced a major cyberattack that resulted in the exposure of sensitive data belonging to around 73 million customers. The breach compromised details like full names, addresses, dates of birth, phone numbers, social security numbers, and AT&T account information. Following the data theft, AT&T took steps to reset account passcodes and provide identity theft protection and credit monitoring services to impacted customers. In response to the incident, a man from Ohio initiated a class action lawsuit against AT&T, alleging negligence and breach of contract.	March 2024

April 2024	Hackers attacked El Salvador’s national cryptocurrency wallet Chivo and exposed over 144 GB of sensitive personal information of millions of Salvadorians. The hackers also released Chivo’s source code publicly. The Salvadorian government has not released an official public statement on the attack.

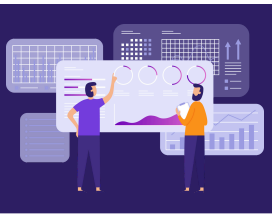
Ticketmaster, an American company specializing in ticket sales and distribution, operates in various countries. From April 2 to May 18, a cyber attack targeted Ticketmaster, leading to the exposure of payment information and personal data of around 560 million customers. Around a week after the incident, on May 28, 2024, the hacking group Shinyhunters took credit for the breach and demanded a $500,000 ransom through the online platform BreachForums. Threat Actor: ShinyHunters	May 2024

June 2024	South Africa's National Health Laboratory Service (NHLS) has reported a ransomware attack that has had a major impact on the distribution of laboratory results during the country's response to an outbreak of mpox. According to a spokesperson for the NHLS, hackers removed portions of their system, including backup servers, necessitating the reconstruction of many affected areas.

A global IT outage, which disrupted airline and hospital operations, was caused by a faulty software update for Microsoft Windows released by cybersecurity firm **CrowdStrike**. Approximately 8.5 million machines were affected, leading to a reported $5.4 billion in damages for Fortune 500 companies.	July 2024

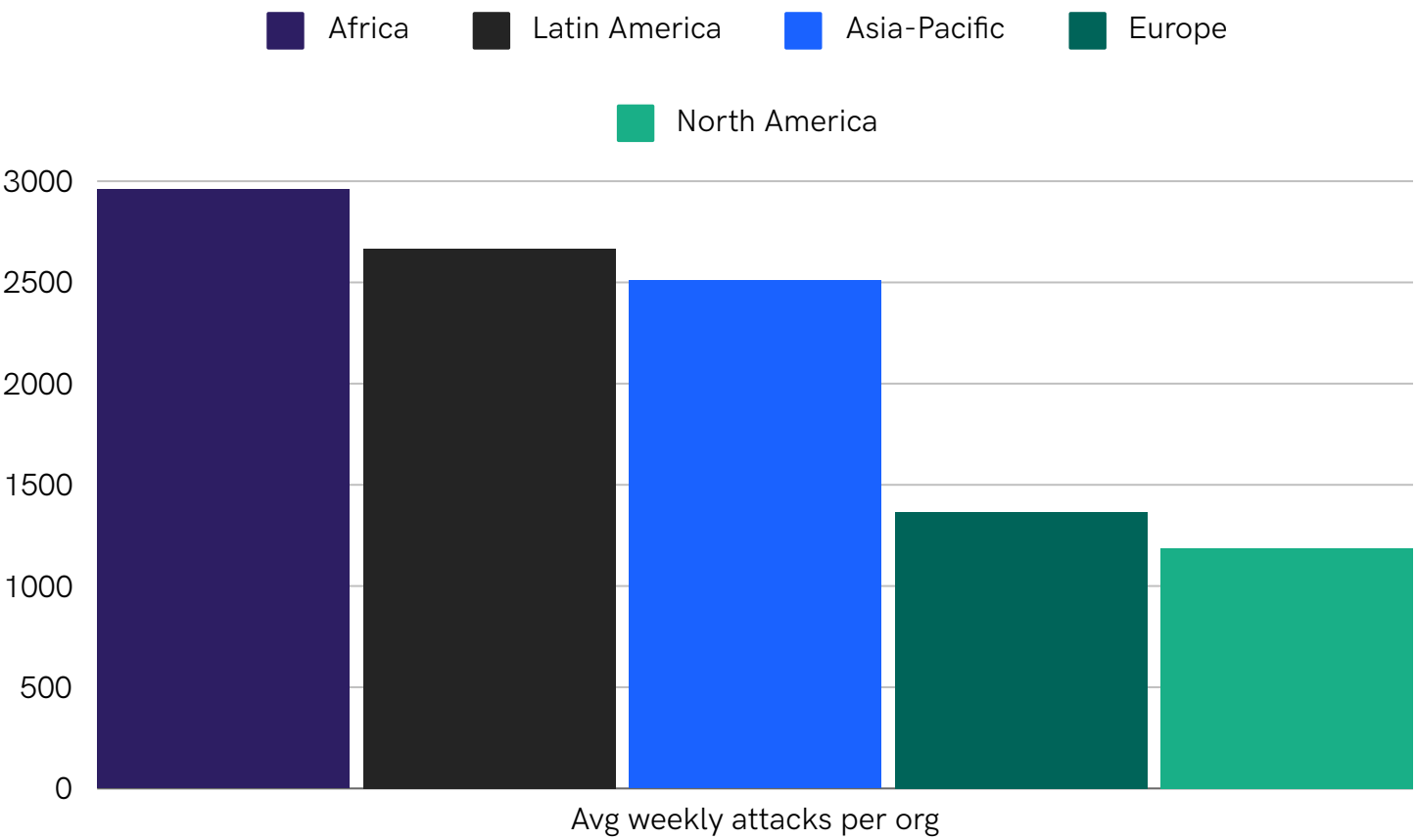
August 2024	Cryptocurrency hackers allegedly hacked into McDonald’s official Instagram account, promoting a fake digital currency, and making off with $700,000 in stolen money. They claim to have targeted McDonald's social media account to promote a fake meme coin called "GRIMACE" on the Solana network. McDonald’s said in a statement it was “aware of an isolated incident that impacted our social media accounts earlier today.”

2024 Cyber Trends



In Q2 2024, Check Point Research saw a 30% Year-on-Year (YoY) increase in cyber attacks globally, reaching 1,636 attacks per organization per week.

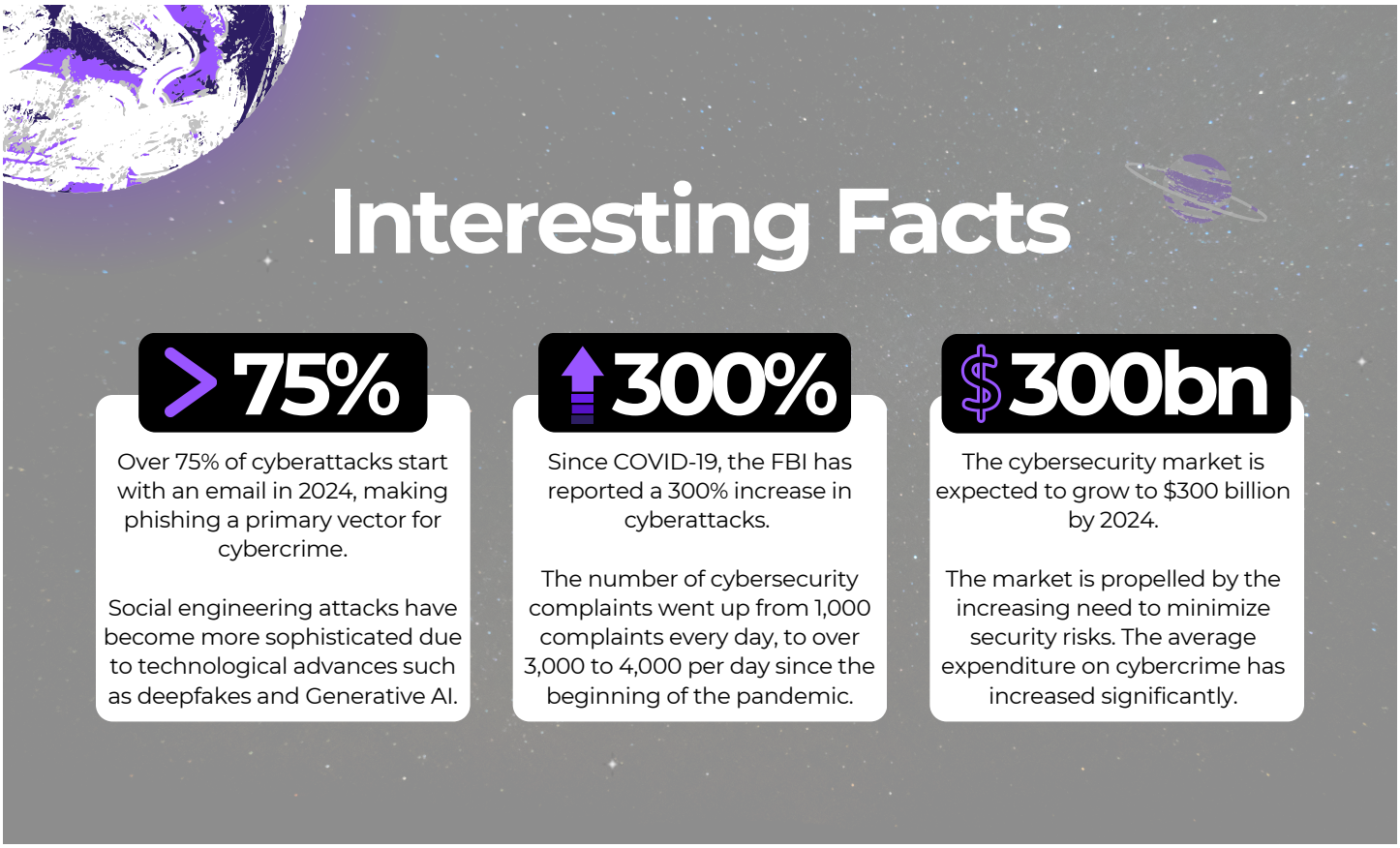
Regional Analysis of Cyber Attacks



Africa had the highest average weekly cyberattacks per organization, with an average of **2,960 attacks**, representing a **37% increase** compared to the same period in 2023. Latin America experienced the most significant rise, with attacks increasing by 53% year-over-year to an average of 2,667 per week. The Asia-Pacific (APAC) region followed with a 23% increase, indicating the global spread of cyber threats.

The Manufacturing sector bore the highest impact, with 29% of global victims of publicly reported **ransomware attacks**, showing a substantial 56% increase year-over-year. Following closely, the Healthcare sector accounted for 11% of the attacks and saw a 27% rise. Retail/Wholesale witnessed 9% of the attacks, marking a significant 34% decrease from the previous year. Interestingly, the Communications and Utilities sectors faced significant spikes in ransomware incidents, with increases of 177% and 186%, respectively.

Interesting Stats



Other cybersecurity statistics include:

Industry:

- Information security jobs are projected to **grow by 32% between 2022 and 2032.**
- **93% of organizations** expect to increase cybersecurity spending over the next year.
- The global cybersecurity workforce is estimated to be around 4.7 million people.
- The total cost of damages incurred by cybercrime is expected to reach **$10.5 trillion by 2025.**

Threats:

- Cloud environment intrusions increased by 75% over the past year.
- 70% of organizations have users being served malware ads on their browsers.
- In just the first 6 months of 2023, ransomware extortion totalled $176 million more than in all of 2022.
- **Business email compromises (BEC)** accounted for over $2.9 billion in losses in 2023.
- **349,221,481 people** were impacted by data breaches in 2023.

Top 10 Cybersecurity Trends

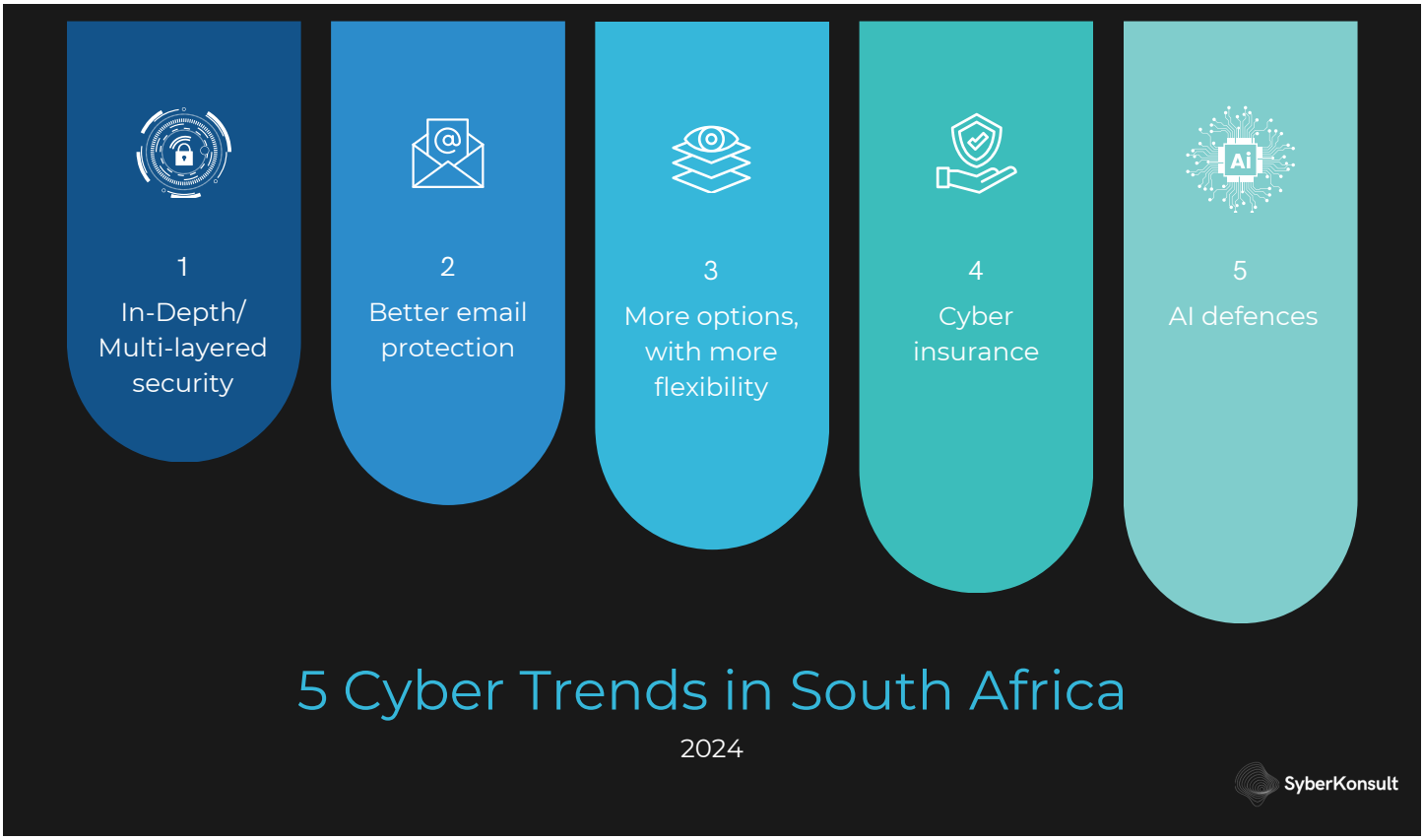
As we come close to the end of 2024, the field of cybersecurity is on the verge of significant changes. Cyber threats are not only increasing in frequency but also growing more sophisticated, challenging traditional security methods. In this rapidly changing digital environment, it's important to anticipate upcoming trends to be prepared.

The challenges posed by modern threats are multifaceted. Individuals face risks of identity theft, financial loss, and privacy breaches. Businesses must contend with the potential for operational disruptions, reputational damage, and significant financial costs associated with data breaches and compliance with regulatory requirements. For governmental bodies, the stakes are even higher, as cyber threats can compromise national security, undermine public trust, and disrupt essential services.

To mitigate these risks, a multi-layered approach to cybersecurity is essential. This includes implementing robust encryption methods, regular security audits, and fostering a culture of cybersecurity awareness. Collaboration between the public and private sectors, along with international cooperation, is crucial in developing comprehensive strategies to combat the ever-evolving digital threat landscape.

South Africa’s Cyber Posture

South Africa's vulnerability stems from affordability challenges, impacting security investments. Economic constraints lead to cost-cutting on security measures, leaving businesses exposed. Watch for five major trends in 2024 as the nation bolsters defences.



1. Multilayered security combines various measures like firewalls, encryption, access controls, behavioural analytics, and endpoint protection to strengthen defences against breaches.
2. Between 90-95% of all security breaches happen through email.
3. Vendors now offer flexible security contracts with monthly payments and scalable products for easier integration and adjustments.
4. Cyber insurance products are increasingly essential as threat vectors rise and more companies face ransom demands from attackers.
5. The proactive approach to combat cyber threats includes adopting diverse security measures, improving email protection, having flexible vendor choices, utilizing cyber insurance, and implementing AI in defence strategies.

South Africa Is No Stranger To Cyber Incidents

The number of cybercrime incidents in South Africa has been on the rise. Notable incidents include a ransomware attack on Johannesburg's electricity utility, City Power, in 2019, and a cyber attack on Life Healthcare Group in 2020. In the same year, a South African credit agency experienced a major data breach, compromising the information of 24 million people. In 2021, a cyber attack on Transnet, a state-owned rail, port, and pipeline company, caused significant disruption to transportation and economic harm. Additionally, ransomware incidents were reported in the Department of Justice and Constitutional Development, affecting the department's systems and services. In August 2023, the South African National Defence Force (SANDF) reported a potential massive data breach. Experts warn that cybercrime incidents are expected to continue rising due to South Africa's weak cybersecurity and poor cyber hygiene.

5th

South Africa was ranked 5th in the cybercrime density list. This list represents the number of cybercrime victims per 1M internet users

R49m

The average cost of a cyber security breach is around R49 million, which is an 8% increase from 2022.

61%

The most common method of attack used by cyber criminals targeting companies is email phishing (61%)

In South Africa, 45% of data breaches stem from criminal attacks, 30% from human error, and 25% from technical glitches. Surprisingly, despite the high likelihood of data breaches, only 35% of companies have a sufficient cybersecurity strategy established.

Understanding the threat of cybercrimes and having a robust cybersecurity strategy is crucial in today's digital landscape. Here are some key steps to enhance your cybersecurity measures:

- Engage cybersecurity professionals or seek assistance from experts in the field.
- Provide training for your staff.
- Regularly review access to sensitive data.
- Implement a response plan to mitigate cyber threats.

By taking these proactive measures, you can fortify your business against the impact of cybercrimes.

Assess your cyber risks, put your response plan into action, and explore the available protection options now to safeguard your business from digital crimes.

SyberKonsult

Email us at:
aya@syberkonsult.co.za

Visit our home on the web at **www.syberkonsult.co.za**!

On social platforms:

Instagram: @syberkonsult
Twitter/X: @syberkonsult

2024 Cisco Cybersecurity Readiness Index

The State of Global Cybersecurity Readiness addresses the current cybersecurity landscape and assesses how ready organizations are globally to face today's cybersecurity risks.

When assessing global cybersecurity readiness for this Index, only 3% of respondent organizations qualify for the Mature category. Nearly three-quarters (71%) fall in the bottom two categories (Formative, 60% and Beginner, 11%).

In South Africa, 5% of organizations are at the **Mature** stage of readiness, 28% are at the **Progressive** stage, 57% are **Formative**, and 10% are **Beginners**. In terms of the pillars of readiness, we found the strongest performance in Network Resilience and AI Fortification, both with 7% of companies in the Mature category. The lowest levels of readiness were in Cloud Reinforcement and Identity Intelligence, with 4% and 5% of companies ranked as Mature respectively.

Resources

The Cybersecurity Hub

The Cybersecurity Hub operates under the mandate of the National Cybersecurity Policy Framework (NCPF), approved by Cabinet in March 2012. Serving as South Africa's National Computer Security Incident Response Team (CSIRT), The hub aims to create a secure cyberspace for South African residents through collaboration with stakeholders to detect and combat cybersecurity risks.

CSIR Information and Cybersecurity Research

The CSIR Information and Cybersecurity Research Centre focuses on developing home-grown cybersecurity and identity management solutions to protect individuals and technological systems from digital threats and vulnerabilities.

State Security Agency - Computer Security Incident Response Team (CSIRT)

ECS-CSIRT is a registered member of the globally recognised ICT and cyber security organisation known as FIRST (Forum of Incident Response and Security Teams). Their main services cater to government bodies, providing a centralized point for CSIRT services and cyber security assistance.

ECS-CSIRT offers daily ICT Information Security reports to keep users informed about breaches, trends, vulnerabilities, and cybersecurity news.

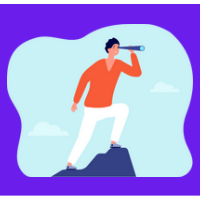
Supplementary Links

Our newest blog posts cover cybersecurity topics specific to South Africa:

Data Privacy Compliance	The State of Cybersecurity in South Africa	Understanding Cybersecurity Compliance in South Africa: A Guide for Businesses

---

What To Look Out For



End the report with an eye toward the future.

- What are the predictions for cybersecurity going forward?
- What does SyberKonsult have in store?

At SyberKonsult, we foresee that the cybersecurity landscape will continue to evolve rapidly, driven by the rise of AI, quantum computing, and the growing sophistication of cybercriminals. As AI becomes more integral to both offensive and defensive strategies, we predict an arms race where cyber threats will be increasingly automated, targeted, and difficult to detect.

Quantum computing poses another looming challenge, with the potential to break traditional encryption methods, necessitating the development of quantum-resistant security protocols.

We also anticipate a shift towards more integrated and proactive security measures, where real-time threat intelligence, automated response systems, and continuous risk management become standard practices. Organizations will need to adopt a more holistic approach to cybersecurity, considering not just technology but also human factors, **governance**, and **compliance**.

Blockchain security will likely play a significant role in this evolving landscape. The decentralized nature of blockchain technology offers enhanced security features that can protect against data breaches and unauthorized access. By ensuring that data is distributed across a network of nodes, blockchain can provide robust protection against tampering and fraud.

Blockchain's transparency and immutability can enhance compliance and audit processes for regulatory requirements. Understanding blockchain security nuances and implementing strategies is crucial for leveraging its strengths.

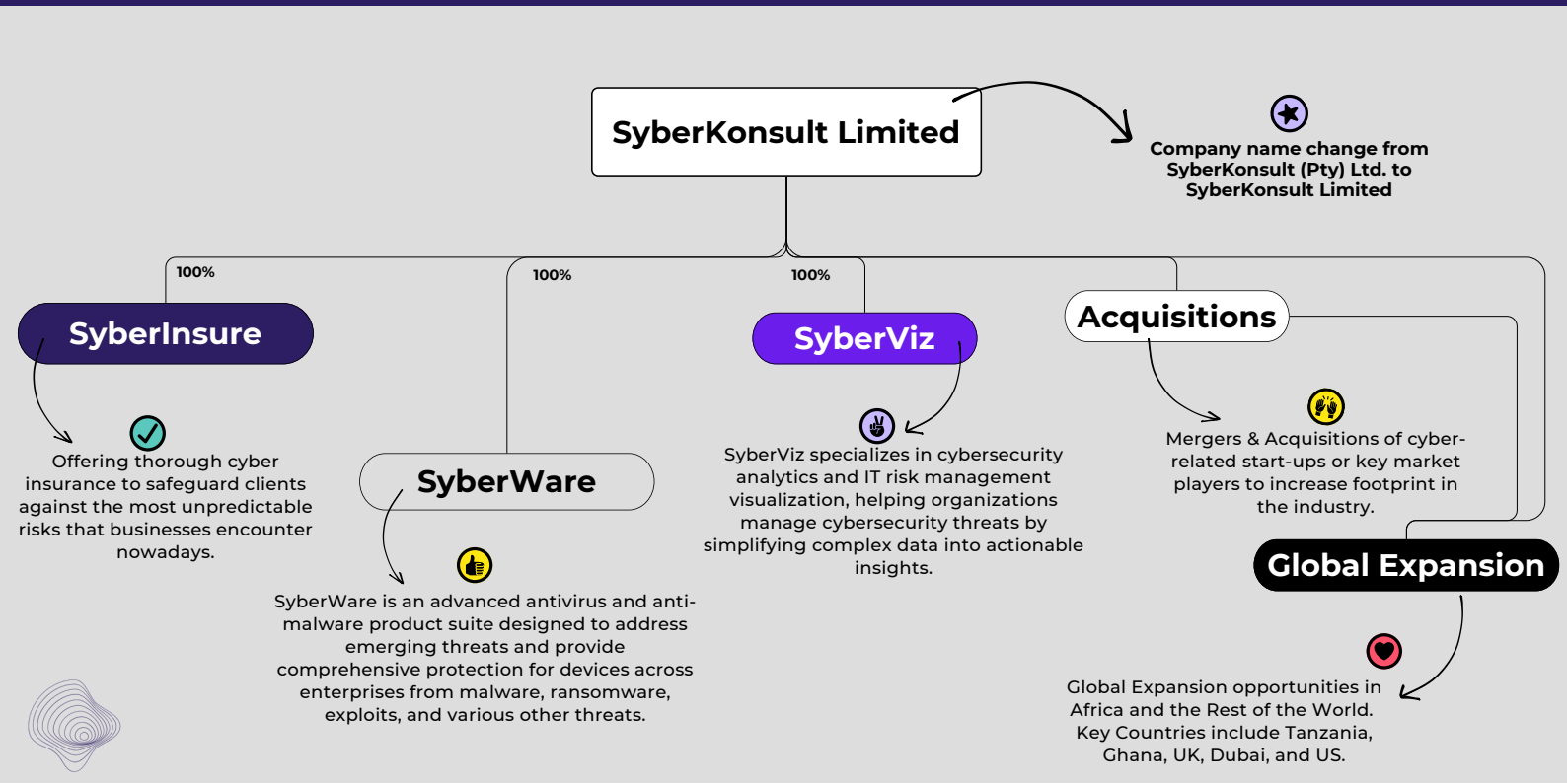
Ultimately, the future of cybersecurity lies in the seamless integration of these innovative technologies with comprehensive security policies and practices.

We are committed to staying ahead of these trends, providing our clients with the cutting-edge tools and strategies needed to navigate the future of cybersecurity. Our dedicated team of experts continuously monitors the evolving landscape, ensuring that we are always one step ahead.

Moreover, our holistic approach encompasses not only technical solutions but also comprehensive training programs to empower our clients' workforce, making them the first line of defence against cyber attacks. With a strong focus on innovation and resilience, we aim to build a safer digital world for everyone.

To enhance and broaden our service portfolio, we are strategically restructuring the company's organizational framework. We look forward to revealing the updated structure and upcoming initiatives illustrated in the diagram below.

Upcoming Structure



Contact Us

For further information, please reach out to us at **aya@syberkonsult.co.za**

SyberKonsult (Pty) Ltd.

Address: 25 Fredman Drive, Sandton, 2191

Phone: 082 390 7785

Website: www.syberkonsult.co.za

SyberKonsult
Security. Intelligence. Governance.

Thanks to our clients and readers.

2024 Cybersecurity Report

The SyberKonsult Team appreciates your time in reading the report. We eagerly anticipate your feedback and exploring potential future collaborations.

Stay safe and secure.

Sources/Credits:

- Tarsus On Demand - What to expect from South Africa's cybersecurity landscape in 2024
- SplashTop - Top 10 Cyber Security Trends And Predictions For 2024
- Webopedia - 7 Biggest Cyber Attacks 2024
- Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks