

# Cybersecurity as an Imperative for Growth

In partnership with Omdia

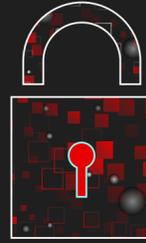
November 2024

OMDIA



vodacom  
business

# Contents



Introduction .....	03	Understanding what cybersecurity affects .....	32
What's the problem? .....	05	4.1 The scope of cybersecurity in an organisation and beyond .....	33
1.1 The scale of cyber-attacks facing South African organisations.....	06	4.2 The core tenets of cybersecurity.....	36
How to think about cybersecurity .....	07	4.3 Cybersecurity as the backbone of resilient digital innovation.....	39
2.1 Cybersecurity as a pillar of digital resilience .....	08	4.4 Cybersecurity as a business enabler: Measuring ROI and long-term value .....	42
2.2 The unchanging nature of the threat .....	10	What organisations need to do .....	44
2.3 Regulation aims to drive enhanced cybersecurity in organisations.....	13	5.1 Know your vulnerabilities.....	45
Understanding the threat .....	15	5.2 Review your cybersecurity controls: People, process and technology .....	47
3.1 How cyber attackers exploit vulnerabilities .....	17	5.3 Evaluate and prioritise your data and systems .....	49
3.2 Ransomware: A growing threat in the digital economy.....	21	5.4 Protect Personally Identifiable Information (PII) from exposure.....	51
3.3 Supply chain attack.....	24	5.5 Conduct regular security assessments and audits .....	52
3.4 Distributed Denial of Service (DDoS) attack .....	26	5.6 Commit to proactive cybersecurity engagement .....	53
3.5 Phishing attack .....	27	5.7 Leverage automation and advanced tools.....	55
3.6 Critical National Infrastructure (CNI) attack.....	28	5.8 Avoid pitfalls of going it alone .....	56
3.7 Next-generation threats: Navigating the future of digital defence .....	29	Conclusion .....	59
		About us .....	60
		Vodacom & Omdia .....	60
		Analyst & Copyright.....	61

# Introduction

**In the pre-digital era, societies developed robust systems—military, law enforcement, education, and legal frameworks—to mitigate vulnerabilities such as greed, malice, negligence, and ignorance. These institutions aimed to preserve stability, enforce accountability, and protect against internal and external threats.**

In today's interconnected digital world, the nature of these threats has evolved, but the need for equally robust defence mechanisms remains. As technology transforms how we live and work, the complexity of digital systems introduces new risks. Cyberattacks are now driven by malicious actors exploiting both human and system vulnerabilities. Just as physical infrastructure once required protection, today's digital infrastructure demands equally rigorous cybersecurity measures.

National cybersecurity strategies, stringent corporate policies, public awareness campaigns, and cross-border collaboration are essential to combat the rising tide of cybercrime. The growing dependency on digital systems—compounded by the proliferation of IoT devices and a global shortage of cybersecurity professionals—intensifies these risks. Legacy systems, human error, and the economic incentives for cybercriminals further amplify the problem.

In this context, cybersecurity is no longer merely a defence mechanism—it is a strategic investment, essential for maintaining stability, fostering innovation, and ensuring business growth. Organisations that prioritise cybersecurity are better equipped to navigate the complexities of today's digital landscape and secure their future.



“

**We are also seeing that cyber security awareness is not prioritised, with only 32% of organisations training their employees”**

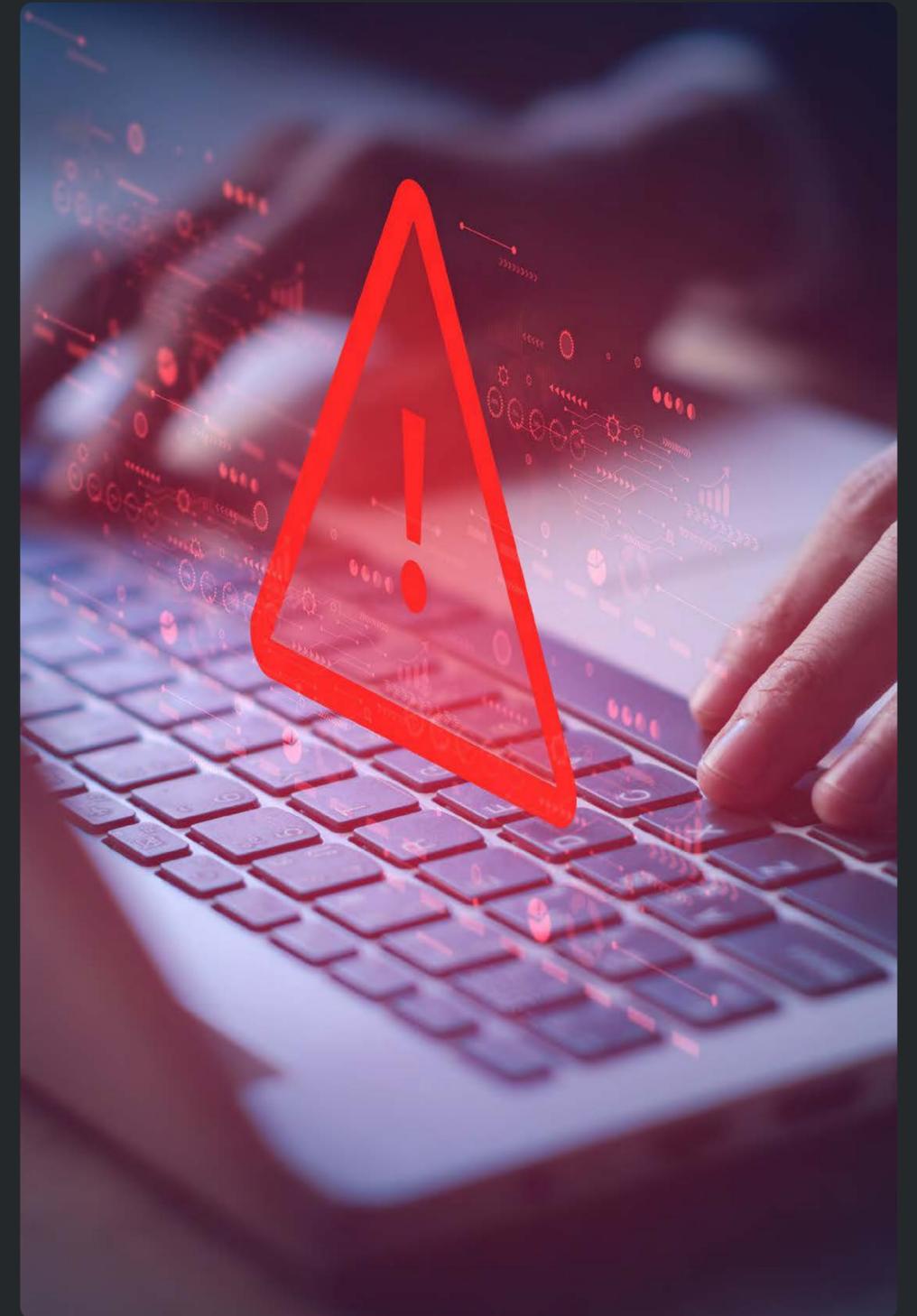
Source: [www.itweb.co.za/article/csir-lifts-lid-on-south-africas-dire-security-posture/xA9PO7NEDAYvo4J8](http://www.itweb.co.za/article/csir-lifts-lid-on-south-africas-dire-security-posture/xA9PO7NEDAYvo4J8)

This thought leadership paper from Omdia and Vodacom Business explores the current state of cybersecurity in South Africa, while also drawing insights from global trends and practices. It has been developed through a blend of primary research, insights from Omdia's IT Enterprise Insights and Cybersecurity Decision-Maker<sup>2</sup> Surveys and expert interviews with cybersecurity experts in South Africa. Among them are individuals who hold prestigious positions, such as the Chair of various cyber industry bodies, and other industry experts. This paper offers actionable recommendations for decision-makers.

By integrating these cybersecurity strategies into their operations, organisations can take advantage of the opportunities in the digital landscape, whilst protecting their brand's reputation. Cybersecurity becomes the strategic enabler for growth. With the right protections in place, organisations can confidently innovate and deliver new digital products and services, secure in the knowledge that their cybersecurity infrastructure is built to support both resilience and progress.

## Key sections of the report cover the following:

- Section **01** Sets the context by looking at the scale of the cybersecurity problem in South Africa and beyond, showing how the country's growth in digital connectivity has made it a focus for global cybersecurity attackers
- Section **02** Provides frameworks for thinking about cybersecurity; why it is central to an organisation's digital resilience; and the importance of meeting regulatory requirements
- Section **03** Outlines how cyber attackers exploit vulnerabilities and what they are looking for when an attack is successful
- Section **04** Looks at the scope and complexity of what cybersecurity covers and the organisational weaknesses that can undermine successful cyber defences
- Section **05** Lays out eight different areas with recommendations for how to tackle the issues raised

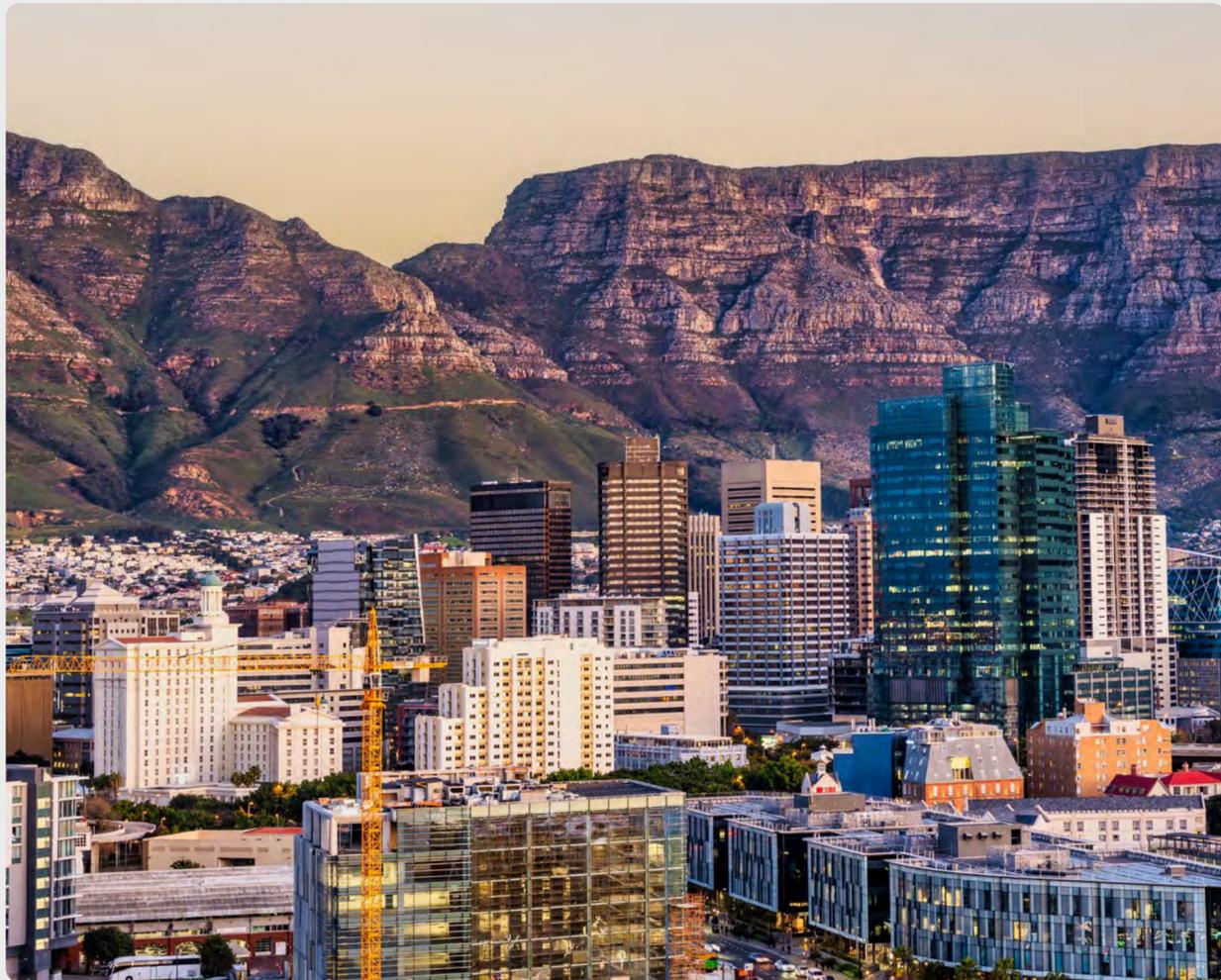


# What's the problem?

# 01



# The scale of cyberattacks facing South African organisations



The cybersecurity threat landscape in South Africa is becoming increasingly dangerous.

**80% of South African businesses reported experiencing a cyberattack in the past year, and SABRIC (South African Banking Risk Information Centre) and CSIR (Council for Scientific and Industrial Research) estimate that the country loses R2.2 billion annually to cyber hacks.**

The country ranks 14th for the highest average insurance claims associated with data breaches and cybercrime, according to a report by Allianz Commercial. The Chair of the Information Regulator stated that 150 data breach notifications are received every month.

Recent South African cyberattacks, as detailed later in this paper, have affected multiple sectors. These incidents caused significant disruption, from interrupting medical operations to preventing citizens from accessing essential utilities. **One of the most notable cases involved hackers stealing over 4TB of data from a South African server and demanding a ransom of US\$15 million.**

In 2023, **South Africa ranked 5th globally for cybercrime victim density.** Reports indicated that 56 out of every one million internet users in the country were victims of cybercrime, placing South Africa among the most affected countries, alongside the US, UK, Canada, and Australia.

<sup>1</sup> Omdia Service Provider Regional Outlook, Africa – Sep 2023)

The digital economy's growth in Africa, particularly in South Africa, is creating more opportunities for cybercriminals. Omdia forecasts Africa's mobile subscriptions to grow from 1.40 billion in 2023 to 1.78 billion by 2028<sup>1</sup>, and **Statista expects internet penetration in South Africa to rise from 75% in 2023 to 98% by 2029.**

Meanwhile, US\$22.53 billion worth of transactions flowed through digital channels in 2023, and the **Mastercard New Payments Index (2022)** found that 95% of South Africans had used at least one emerging payment method two years prior. Online retail in South Africa was worth R71 billion in 2023 and is projected to reach R100 billion by 2026.

Individuals and organisations alike are becoming increasingly dependent on uninterrupted access to digital infrastructure, underscoring the importance of reliable, scalable systems that can meet this growing demand. If this is true for South Africa, it is equally important in those African countries where South African-based businesses have operations.

As Africa's digital economy rapidly transforms and expands, it increases vulnerabilities and provides more entry points for increasingly sophisticated cybercriminals, hackers, and state-sponsored actors. These threat actors use increasingly sophisticated methods to steal data, disrupt services, and cause significant damage to organisations. The frequency and complexity of cyberattacks are accelerating, making it harder for cybersecurity professionals to defend sensitive and confidential information and maintain the integrity of digital systems.

# How to think about cybersecurity

# 02



# Cybersecurity as a pillar of digital resilience

Digital resilience is the capacity of an organisation to maintain continuous operations despite potential disruptions, and swiftly capitalise on digital opportunities.

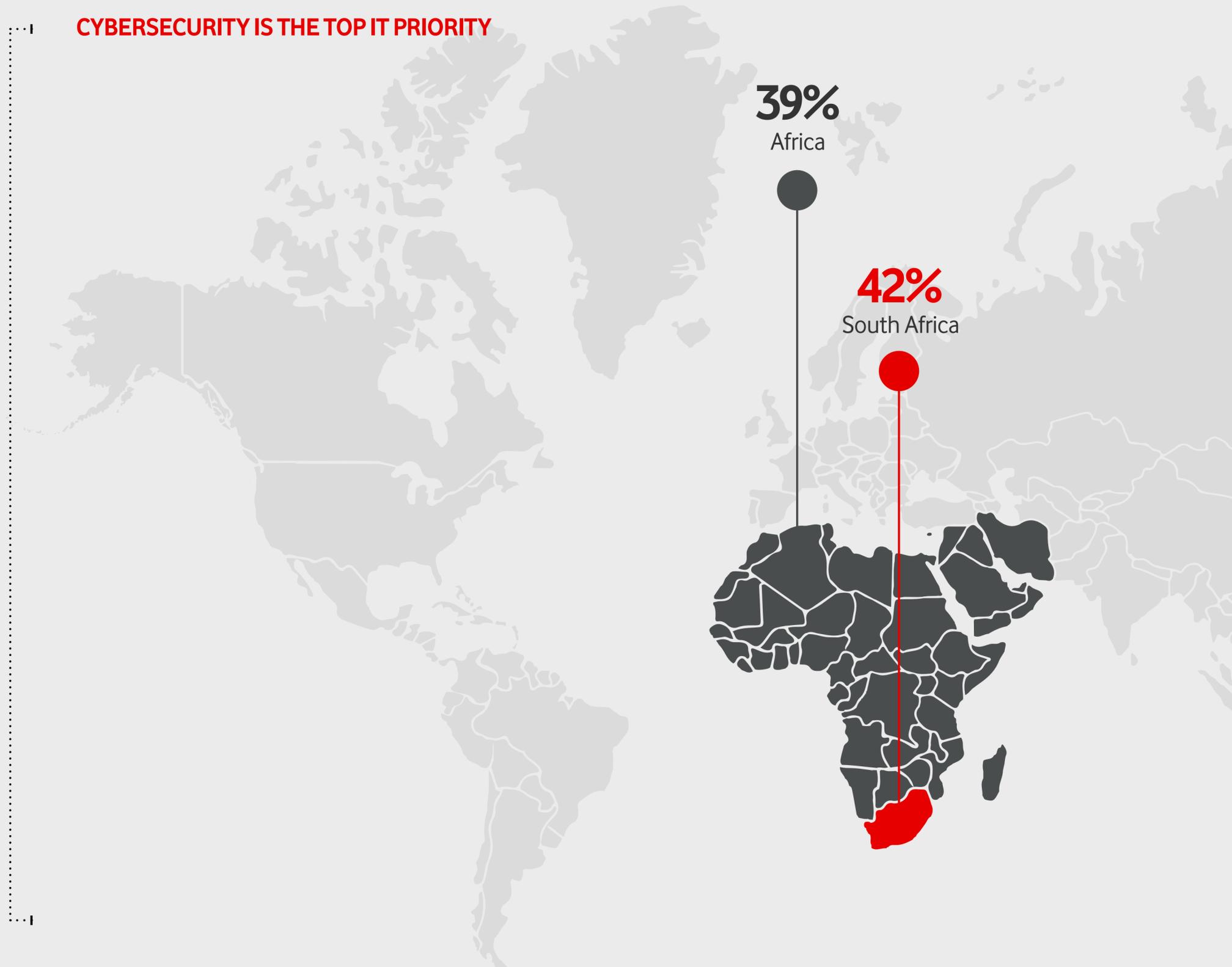
**The cyber-outages on 19 July 2024 that grounded planes, closed banks, and disrupted the online insurance market underscored the importance of digital resilience. These disruptions were caused by third-party software updates.**

To achieve true digital resilience, organisations must prioritise cyber resilience—the ability to withstand, respond to, and recover from cybersecurity threats. According to Omdia's IT Enterprise Insights Survey 2024, 42% of global organisations, including those in South Africa, rank cybersecurity as their top IT priority and all top three IT priorities are related to cyber-security: Cybersecurity, identity and privacy management<sup>2</sup>.

<sup>2</sup> Omdia IT Enterprise Insights Survey 2024-25 n=5099, 389, 131

42% Worldwide

## CYBERSECURITY IS THE TOP IT PRIORITY



“  
If you ask me what keeps me awake at night, and it is a bit of a cliché, it’s definitely cybersecurity because the thing is, you just don’t know. There are probably hundreds, if not thousands of people on a daily basis trying to infiltrate your systems.”

The Group CIO of Standard Bank Jörg Fischer emphasised the ever-present nature of the threat in an interview with Tech Central

Furthermore, only 36% of organisations are confident they can prevent a ransomware attack without significant operational disruption<sup>3</sup>. Many interviewees for this report corroborated this global view, with comments including

“

**“ransomware attacks are often successful in South Africa and organisations are frequently unprepared”.**

Omdia’s Cybersecurity Decision-Maker Survey revealed that 62% of organisations globally reported a significant increase in the severity of cyber threats over the past two years, up from 55% in 2023. Alarmingly, more than half of the respondents faced multiple severe incidents in the past year, which required major escalations and resulted in substantial material impacts. Again, the position in South Africa reflects this global survey, with interviewees noting that ethical lines are being crossed, with attacks on medical facilities as an example.

As cyber threats continue to evolve and become more sophisticated, businesses must continuously adapt their cybersecurity strategies to safeguard their operations.

<sup>3</sup> Omdia Cybersecurity Decision-Maker Survey 2024, n=964

# The unchanging nature of the threat

Cybercriminals are becoming more sophisticated in exploiting system vulnerabilities, with financial gain serving as a key driver behind a wide array of attacks. Economic incentives are increasingly shaping the landscape of cybercrime. Below are key examples of how financial motives influence cybercriminal activity.



## Ransomware attacks

Cybercriminals use ransomware to encrypt an organisation's data and demand payment, often in cryptocurrency, to restore access. The promise of substantial ransoms makes this a highly profitable form of attack.



## Corporate espionage

Cybercriminals may be hired to steal sensitive information from competitors, such as trade secrets or product designs, in exchange for large payments from rival businesses.



## Crypto jacking

Hackers hijack the processing power of infected systems to mine cryptocurrency, benefiting from the resources of compromised computers without the victim's knowledge.



## Money laundering

Cybercriminals often exploit the anonymity of cryptocurrencies to launder stolen money, using complex financial schemes to obscure the origins of their funds and make it harder for authorities to trace.



## Data theft and sale

Personal, financial, or intellectual property data is highly valuable on the dark web. Cybercriminals steal data to sell it to the highest bidder, making data breaches lucrative for those involved.



## Fraud and identity theft

Stolen personal or financial data can be used to commit fraud, such as opening credit accounts or making unauthorised transactions. Cybercriminals can exploit this for financial gain over time.



## Distributed Denial of Service (DDoS) extortion

Cybercriminals launch DDoS attacks to overwhelm a business's online services and demand payment in exchange for halting the disruption, pressuring businesses to pay quickly to minimise operational losses.



## Cybercrime-as-a-Service (CaaS)

The rise of CaaS platforms allows less technically skilled individuals to hire cybercriminals or purchase readymade attack tools, lowering the barrier to entry and enabling more financially motivated attacks.



## Phishing for profit

Phishing schemes are designed to trick individuals into revealing their login credentials, banking details, or credit card information, which cybercriminals then exploit for financial gain.

**The economic incentives for cybercriminals continue to grow as digital assets and online transactions increase in value. Businesses must stay vigilant and implement robust security measures to counter the financial motivations driving these threats**

The rapid expansion of IoT devices and other connected technologies has significantly increased the potential attack surface for hackers but this evolving threat landscape is compounded by vulnerabilities such as:

## Legacy systems

Often outdated and lacking modern security measures, present several vulnerabilities that can pose significant risks to organisations. Here are some common examples:



### Outdated software and patches

Legacy systems often run on outdated software that no longer receives updates or security patches, leaving them exposed to known vulnerabilities that attackers exploit.



### Insecure interfaces and APIs

Legacy systems often have poorly designed or outdated interfaces that lack proper authentication and security controls, providing attackers with potential entry points.



### Vulnerable to modern attacks

Many legacy systems are not equipped to defend against modern cyber threats such as ransomware, advanced persistent threats (APTs), or zero-day vulnerabilities.



### Hardcoded credentials

Some legacy applications and systems use hardcoded credentials within the code, making them easy targets if attackers gain access to this information.



### Unsupported operating systems

Many legacy systems operate on operating systems that are no longer supported by the vendor (e.g., Windows XP or older Linux distributions), making them susceptible to malware and other attacks.



### Weak authentication mechanisms

Many legacy systems still use weak or outdated authentication methods, such as default passwords, singlefactor authentication, or easily guessable credentials.



### Limited visibility and monitoring

Legacy systems may not integrate with modern security monitoring tools, leaving organisations blind to potential breaches or ongoing attacks.



### Lack of encryption

Older systems may not utilise modern encryption standards for data storage or transmission, increasing the risk of data breaches and unauthorised access.



### No segmentation or isolation

Legacy systems are often part of a flat network, with no segmentation between different parts of the infrastructure, allowing attackers to move laterally once inside.



### Poor integration with newer technologies

As legacy systems often struggle to integrate with newer technologies, this mismatch can create security gaps or overlooked vulnerabilities.



**Addressing these vulnerabilities requires a strategy of upgrading, patching, and, where necessary, replacing legacy systems with modern, secure alternatives.**

## Human error

Remains one of the most significant vulnerabilities in any organisation's cybersecurity framework and was frequently referred to by the cybersecurity experts interviewed for this report, including that **“there are many accidental issues”** and **“social engineering is a key focus for attackers”**. Below are common examples of how human mistakes can expose businesses to risk



### Weak passwords

Employees may use weak, easily guessable passwords or reuse the same password across multiple systems, making it easier for attackers to gain access to critical information.



### Accidental data sharing

Employees may unintentionally share sensitive information through unsecured channels, such as personal emails or cloud storage services, increasing the risk of data leaks.



### Unintentional data deletion or modification

Mistakes in data handling, such as accidentally deleting or modifying important files, can cause operational disruption or data loss.



### Insufficient awareness of security protocols

Without regular training, employees may not fully understand the importance of adhering to security policies, leading to careless actions such as downloading unapproved software or connecting to insecure networks.



### Phishing attacks

Staff can inadvertently fall victim to phishing scams, clicking on malicious links or attachments that give attackers access to internal systems or sensitive data.



### Failure to install security updates

Users may neglect to install critical security updates or patches, leaving systems vulnerable to known exploits that attackers can leverage.



### Improper use of privileged access

Employees with elevated privileges may misuse or mishandle access, whether through negligence or lack of knowledge, potentially leading to a breach.



### Misconfiguration of systems

Errors in the setup or configuration of security systems, such as firewalls or cloud services, can create vulnerabilities that hackers can exploit.



### Inadequate handling of credentials

Poor management of login credentials, such as writing down passwords or sharing accounts, weakens the organisation's security posture.



### Lack of incident reporting

In some cases, employees may fail to report a potential security issue, such as a suspicious email or a mistake they made, allowing vulnerabilities to persist and escalate.



**Addressing human error requires ongoing training, strong security policies, and a culture of vigilance to ensure that employees remain aware of their role in safeguarding the organisation from cyber threats.**

# Regulation aims to drive enhanced cybersecurity in organisations

To prevent vulnerabilities, regulations like South Africa's Protection of Personal Information Act (POPIA) aim to ensure organisations take reasonable steps to prevent cybersecurity breaches.

POPIA, overseen by the Information Regulator, defines personal information as data relating to a living person or an existing company, and mandates that this data is processed and stored only as long as necessary. The Act is grounded in eight core conditions, ranging from accountability and security safeguards to openness and data subject participation—all designed to ensure that organisations responsibly manage sensitive data.

POPIA is part of a broader trend. Globally, regulations like the European Union's General Data Protection Regulation (GDPR), which inspired similar laws such as Kenya's Data Protection Act (DPA) of 2019, are setting new standards for data protection. According to interviews, the threat of significant fines for cybersecurity lapses

For organisations that are identified as critical national infrastructure, such as financial institutions, the requirements go even further. In South Africa, financial institutions must comply with the Cybersecurity and Cyber Resilience Requirements set by the Financial Sector Conduct Authority (FSCA) and the South African Reserve Bank (SARB) by June 2025. Similarly, communications providers and other industries must meet the stipulations of the Cyber Crimes Act to maintain regulatory compliance.

For companies found in breach of regulations, penalties are severe and increasing. Under POPIA, for example, serious violations can result in fines of up to R10 million or imprisonment for up to 10 years. In 2023, the Department of Justice and Constitutional Development (DoJ&CD) was fined ZAR5 million for failing to comply with an enforcement notice—a clear example of the regulatory muscle behind these laws and the costs of not complying. Interviewees for this paper were positive about the impact of regulation in driving more recognition of and action around cybersecurity.

Multinational companies and organisations based in South Africa are affected by three different layers of data privacy regulation: GDPR from the European Union and UK, South African domestic requirements, and African country regulation like Kenya's DPA. Organisations must not only comply with current requirements but also proactively adapt to the evolving regulatory landscape. By doing so, they can better secure their operations, protect their data, and ensure compliance—fortifying their defences in an increasingly hostile digital environment.

It is important to stay ahead of regulation for, as one major regional company executive interviewed commented:

**“Regulation often lags behind technological advancements, so maintaining a proactive approach is crucial for staying ahead of threats. Companies should aim to be ahead of the curve by exceeding regulatory standards and focusing on their reputation for security and privacy.”**



# Understanding the threat

035



# Understanding the threat

**Cyberattacks have evolved into one of the most pressing threats to global cybersecurity, impacting not just individuals and businesses, but also governments and critical infrastructure. Globally, over one-third of organisations suffered cybersecurity breach events costing over \$0.5m to address<sup>4</sup>, and IBM reports that the average cost of a data breach is US\$4.88m in 2024, up from US\$4.45m in 2023<sup>5</sup>. This same report notes that malicious attacks accounted for 55% of breaches, and 23% were a result of IT failures.**

Omdia's Cybersecurity Breaches Tracker noted that of 1,307 separate reported breaches globally in 2023, over 69% resulted in data exposure. The sophistication and diversity of these attacks highlight the different motivations that drive malicious actors, from espionage and financial gain to disruption and power demonstration. The threat is significant, and organisations must do what they can to mitigate these threats.

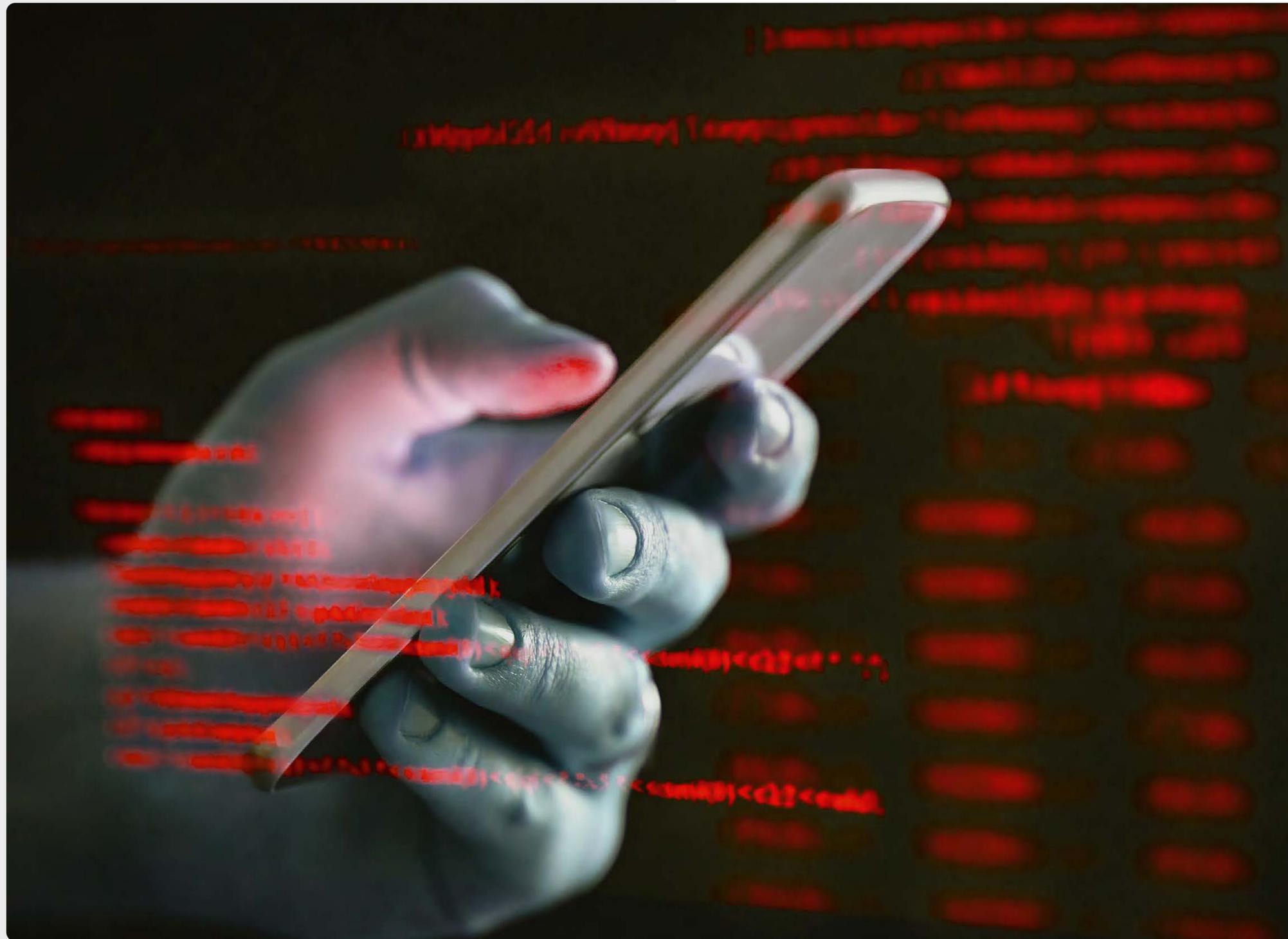
In some of the most significant breaches of the past decade, attackers have exploited vulnerabilities in supply chains, leveraged third-party access, taken advantage of digital projects opening new attack vectors, and even caused physical disruptions like power blackouts. For example, the Trend Micro mid-year cybersecurity threat report 2024 notes that risky cloud app access is the leading risk event during the first half of the year<sup>6</sup>. These breaches show that cybersecurity threats are multifaceted, affecting not only data but also the operational capabilities of major entities.

<sup>4</sup> Omdia Cybersecurity Decision-Maker survey 2024, global, n=964

<sup>5</sup> IBM and Ponemon Institute "Cost of a Data Breach" report, 2024

<sup>6</sup> Trendmicro.com





## How cyber attackers exploit vulnerabilities

**There are a huge variety of cyber threats dominated by highly organised groups leveraging advanced technologies to exploit vulnerabilities.**

These range from automated system scanning to more sophisticated techniques involving artificial intelligence (AI), which enables attackers to identify weaknesses more quickly and efficiently.

For example, comments from interviewees for this report included:

“

**Attackers keep changing their tactics– phishing has evolved through WhatsApp, Instagram, SMS, and more”; “ransomware is very focused on stealing data and holding it to ransom”; and “small organisations are more interested in cost than cybersecurity, leaving them open to evermore attacks.”**

## CYBER ATTACKERS GENERALLY FALL INTO TWO CATEGORIES:

### SOPHISTICATED OPERATORS

1



## WHO EXPLOIT INTRICATE SYSTEM VULNERABILITIES

Globally, ransomware has caused widespread disruption, a strong example of which is the infamous WannaCry attack of 2017. This attack affected more than 250,000 computers across 150 countries, exploiting a vulnerability in Microsoft Windows. Victims included the UK's NHS, FedEx, Renault, Deutsche Bahn, Telefonica, Hitachi, and even the Chinese Ministry of Public Security, leading to cancelled medical appointments, delayed shipments, and operational disruptions.

WannaCry's method of attack involved tricking users into opening malicious emails, which unleashed a self-replicating worm, causing widespread disruption.

The attack held critical systems hostage for ransom, resulting in estimated damages of up to \$8 billion globally. More alarming, however, were the implications—WannaCry exposed how vulnerable essential institutions are to sophisticated cyberattacks.

Ultimately, the situation was mitigated by a fortunate discovery. A 22-year-old British security researcher, Marcus Hutchins, identified a kill switch embedded within the malware's code. By purchasing an unregistered domain linked to the virus's control structure for just \$10.69, Hutchins effectively halted.

### OPPORTUNISTIC ATTACKERS

2



## WHO PREY ON OBVIOUS WEAKNESSES IN BASIC CYBERSECURITY PRACTICES

**The Postbank data breach** in 2020 saw over **R56 million** stolen due to compromised internal controls. Hackers gained access to the bank's master key, which is used to encrypt transactions and generate account information. The master key was not properly secured, allowing fraudsters to use it to carry out fraudulent transactions, particularly affecting social grant recipients.

This breach highlighted significant flaws in Postbank's cybersecurity, such as inadequate cryptographic key management, poor internal monitoring, and a delayed response to the incident. As a result, Postbank was forced to replace millions of bank cards, costing the organisation significantly and damaging public trust.

This incident serves as a cautionary example of how fundamental cybersecurity failures can lead to major financial and reputational damage. However, external threats are only part of the challenge. Insider threats pose significant risks to organisations. There are three key types of insider threats:



## ACCIDENTAL INSIDER THREATS

These occur when individuals unintentionally expose vulnerabilities due to a lack of awareness or knowledge.

For example, the **Capital One data breach (2019)** was caused by a misconfigured firewall that left sensitive data accessible to hackers. This misconfiguration was quickly exploited by a cybercriminal, who accessed personally identifiable information (PII) provided by Capital One customers. Preventing such accidents requires continuous security training and the use of automated tools to detect misconfigurations.

**In 2022, TransUnion, a major credit bureau operating in South Africa, faced a significant data breach**, marking one of the country's most high-profile cybersecurity incidents. The breach exposed personal

information of millions of South Africans, raising concerns about the security of sensitive financial and personal data. The incident was a result of both external hacking and internal vulnerabilities, with reports indicating that employee-related errors played a key role in allowing hackers to gain unauthorised access.

This breach underscores the dual nature of insider threats, which can arise either through malicious intent or accidental actions by employees. In this case, weaknesses in how employees managed or protected critical information contributed to the vulnerability, which hackers exploited to penetrate the system.

The TransUnion breach served as a stark reminder of the importance of robust cybersecurity practices, particularly in organisations that handle large volumes of sensitive data. It also emphasised the need for ongoing employee training and awareness programs to ensure that staff are equipped to handle data securely and avoid errors that could lead to breaches. This incident highlighted the intersection of human error and cybersecurity risks, demonstrating the need for a holistic approach to data protection.

For South Africa, this breach had wide-reaching implications, influencing both regulatory scrutiny and public trust in how businesses manage sensitive information.



## NEGLIGENT INSIDER THREATS

These occur when individuals knowingly disregard security protocols. A notable example is the **Facebook-Cambridge Analytica scandal**, where employees failed to enforce data protection policies, allowing unauthorised access to data. Even though cyber criminals did not directly exploit this situation, it caused significant damage to Facebook's reputation, and Cambridge Analytica was dissolved as a company. Organisations must enforce stricter policies and conduct real-time monitoring to prevent negligence.

**A notable South African example of a negligent insider threat occurred with Liberty Holdings, a major financial services company, in 2018.**

In this incident, Liberty fell victim to a data breach caused by the failure to adequately protect its systems from vulnerabilities, despite internal knowledge of the risks. Although cybercriminals were involved in the attack, the breach was exacerbated by employee negligence, as internal staff did not adhere to or enforce the necessary security protocols that could have prevented the attack.

The breach exposed sensitive personal and financial information of clients, causing significant reputational damage to Liberty. The company faced public scrutiny for not safeguarding its customers' data effectively, even though the

breach was not directly caused by malicious insiders.

This example highlights the risks of negligent insider threats, where employees fail to follow or enforce security measures, leading to vulnerabilities that can be exploited by external actors. As with the Facebook-Cambridge Analytica scandal, the damage in this case was reputational, with trust in Liberty eroded. It underscores the importance of enforcing stricter data protection policies and real-time monitoring to detect negligence before it results in a breach.



## MALICIOUS INSIDER THREATS:

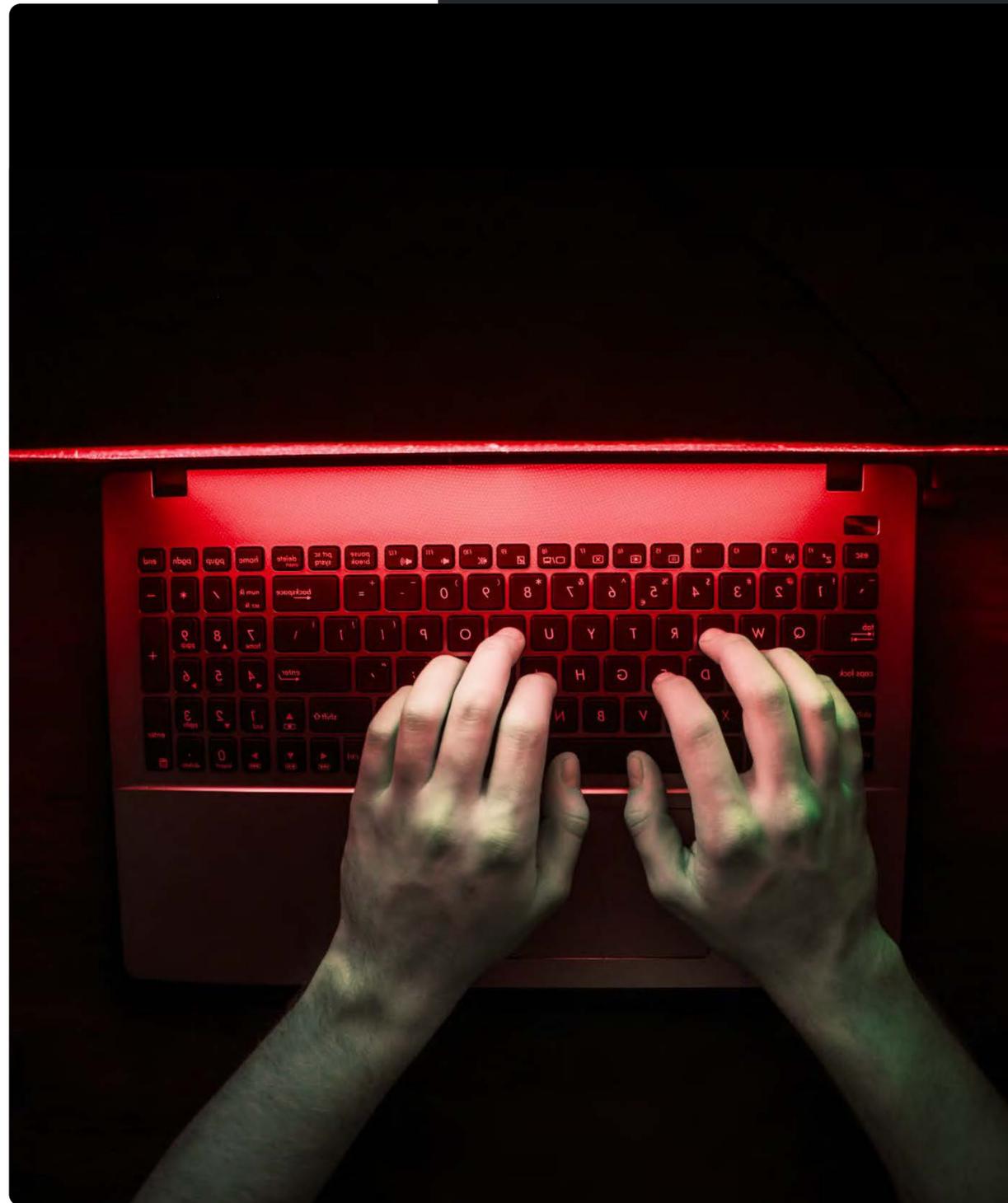
These occur when individuals intentionally cause harm, often for financial gain, ideological reasons, or personal grievances. **The Edward Snowden leak (2013)** is a prime example, where a contractor for the United States National Security Agency (NSA) deliberately leaked classified information. Organisations can mitigate this risk by implementing stringent access controls, conducting background checks, and continuously monitoring privileged accounts.

**The South African Post Office (SAPO) was involved in a significant insider cybersecurity breach**, where a former employee collaborated with external cybercriminals to exploit the organisation's internal systems. With insider knowledge of SAPO's infrastructure, the ex-employee played a pivotal role in bypassing security measures, enabling unauthorised access to sensitive customer data.

This breach underscores the dangers of insider threats, particularly when employees with detailed system knowledge intentionally abuse their access. In this case, the insider's actions were crucial in undermining SAPO's security, demonstrating that even well-protected organisations are vulnerable when trusted individuals act maliciously.

The incident highlighted the importance of strict internal controls, such as regular monitoring of employee access to sensitive or confidential information, conducting thorough background checks, and ensuring former staff cannot access critical systems after leaving the organisation. It also reinforced the necessity of continuous auditing, careful segregation of duties, and robust security protocols to detect and prevent insider threats.

Ultimately, the SAPO breach revealed that insider threats, especially when combined with external criminal networks, can result in severe financial and reputational damage, further underscoring the need for strong cybersecurity measures that address both external and internal risks.



**Organisations must account for both external and insider threats, as these risks can combine to severely compromise an organisation's security.**

Interviewees consistently highlighted the human factor as a significant challenge and highlighted the need to empower people to understand their role in security. As one cyber-security expert said when interviewed:

**“Human error and negligence are major contributors. Common issues include poor credential management, lack of cybersecurity awareness, and inadequate training.”**

While there is no exact percentage that pinpoints human error as the primary cause of cyberattacks, the fact remains that many incidents stem from accidental or negligent actions by users, whether they are internal or external to the affected organisation. IBM's Cost of a Data Breach Report 2024 suggests that 22% of root causes of data breaches are because of human error. Even well-meaning employees can fall prey to phishing schemes, which are often the starting point for more destructive attacks like ransomware.

By taking a proactive approach to insider threat management, organisations can minimise the risks posed by accidental, negligent, and malicious insiders, securing their operations and data. (see section 5.5)



# Ransomware: A growing threat in the digital economy

**Ransomware is one of the most severe threats facing organisations today, and every organisation should expect repeated attempts at such attacks. Omdia's Cybersecurity Breaches Tracker notes that in 2023, 15% of all attacks were ransomware focused, and 2024 numbers are following a similar pattern<sup>7</sup>.**

According to Trend Micro's mid-year cybersecurity threat report 2024, banking was the leading sector subjected to ransomware attacks, followed by technology and then government<sup>8</sup>.

Attackers use ransomware to encrypt files and demand a ransom payment for their release. Often, attackers employ "double extortion" tactics, threatening to publish stolen data if the ransom isn't paid. This type of attack can result in operational disruptions, financial losses, and severe reputational damage. According to Omdia's Cybersecurity Decision Maker Survey 2024, 41% of organisations globally have ransomware in their top three challenges facing the security function.

Each industry faces unique ransomware threats driven by its operational structure, the sensitivity of its data, and the complexity of its technology environment. According to Zscaler's ThreatLabz 2024 Ransomware Report, industries such as manufacturing, healthcare, technology, education, and financial services are among the most frequently targeted by ransomware attacks.

<sup>7</sup> Omdia Cybersecurity Breaches Tracker, 1Q24

<sup>8</sup> Trendmicro.com

# Several notable ransomware attacks have hit South Africa, including



**YEAR**  
**2019**

## EVENT

Johannesburg's electricity provider suffered a ransomware attack that prevented customers from purchasing prepaid electricity, impacting 250,000 customers and delaying responses to power outages. The attack caused significant operational disruptions and raised concerns about the vulnerability of utility providers to cyber threats.



**YEAR**  
**2020**

## EVENT

One of South Africa's largest private healthcare providers faced a ransomware attack that disrupted its IT systems, forcing 66 hospitals to revert to manual processes and impacting patient care. The attack affected service delivery and patient care, highlighting the potentially life-threatening consequences of ransomware attacks in healthcare.



**YEAR**  
**2024**

## EVENT

National Health Laboratory Service (NHLS) (2024): The NHLS, which provides diagnostic services for 80% of South Africa's population, was attacked by the Black Suit ransomware group. The attack disrupted the processing of over 6.3 million bloodtests, delaying critical diagnoses for diseases like HIV and tuberculosis. With system backups deleted, the organisation faced significant challenges in restoring operations.



**YEAR**  
**2019**

## EVENT

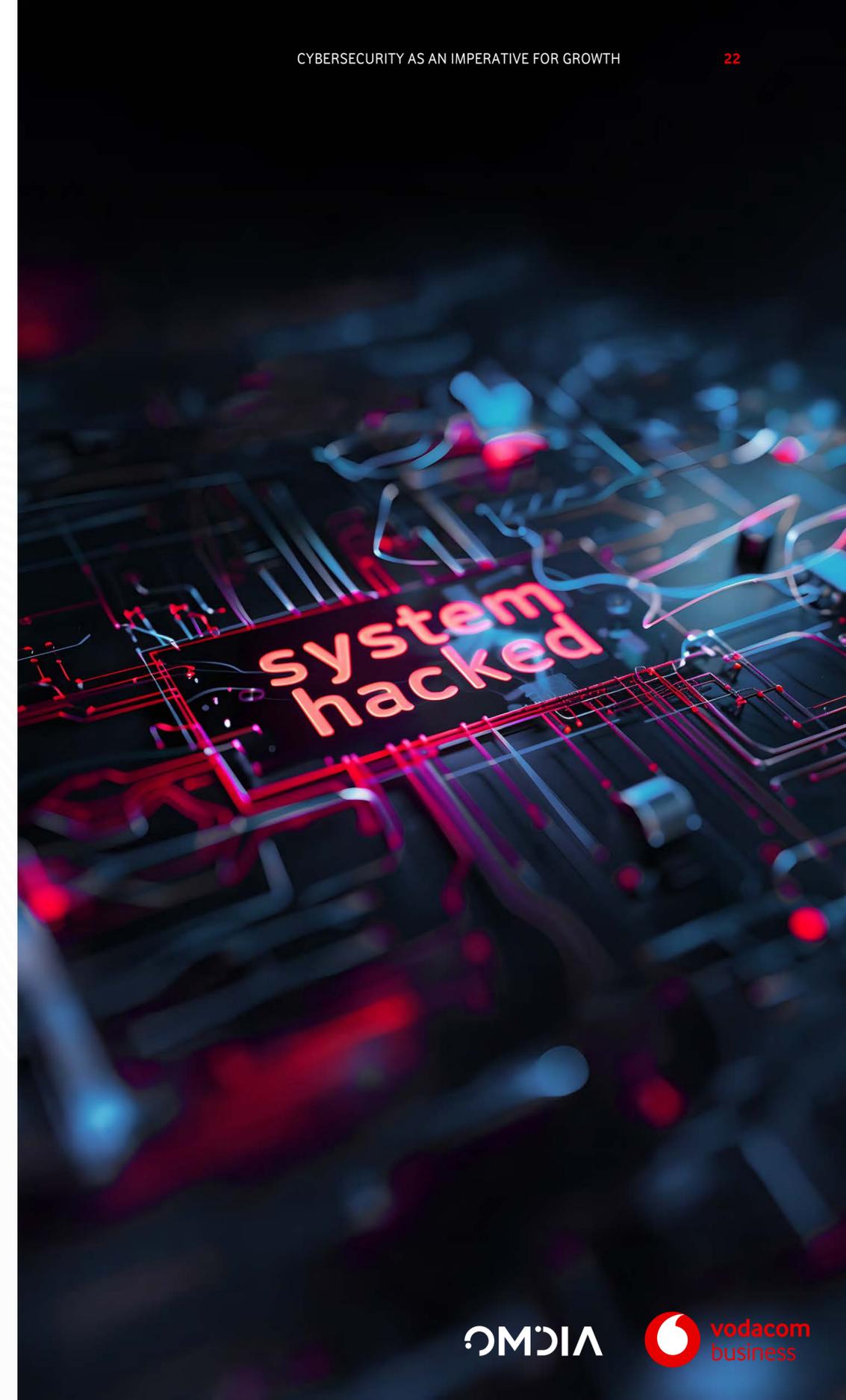
The Shadow Kill Hackers targeted the city's municipal government, encrypting critical data and demanding a ransom. This attack led to a shutdown of the city's online services, affecting billing platforms for water, electricity, and property taxes.



**YEAR**  
**2023**

## EVENT

The Akira ransomware group targeted the Development Bank of Southern Africa (DBSA), encrypting key servers and threatening to publish sensitive financial and personal data. This attack illustrates how financial institutions are increasingly at risk from sophisticated ransomware groups.



Today, ransomware remains a growing and evolving threat, particularly with the rise of double extortion tactics that increase pressure on organisations to pay ransoms both to get their data unlocked and to prevent its sale on the dark web. Critical sectors like healthcare, utilities, and government are key targets, as attacks can disrupt essential services and expose sensitive data.

Cybercriminals are increasingly utilising Ransomware-as-a-Service (RaaS) platforms, allowing less skilled attackers to launch sophisticated attacks by paying for ransomware kits (a component of cybercrime-as-a-service). Trend Micro highlights that this democratisation of cybercrime is contributing to the sharp rise in ransomware incidents globally, making it crucial for organisations to bolster their defences.

The DarkSide RaaS group was behind the attack on Colonial Pipeline, which led to significant fuel supply disruptions across the East Coast of the U.S. The attackers used the RaaS model to infiltrate the pipeline's network, encrypting critical files, and demanding a ransom to restore access. This incident highlighted the dangerous implications of RaaS on critical infrastructure and prompted stronger cybersecurity measures in industries reliant on operational technology.

To combat this threat, businesses must implement strong IT and cybersecurity defences, including regular backups, multi-factor authentication, and continuous network monitoring. (see sections 5.2-5.4) Research and interviews for this paper, commissioned by Vodacom Business and conducted by Omdia, confirm that vendors and service providers recognise that there is no absolute protection against ransomware attacks, also acknowledged by Trend Micro in its 2024 Cyber Risk Report<sup>9</sup>.

As a result, it is crucial for vendors and service providers to support their customer organisations to be fully prepared for such incidents and mitigate their impact to the greatest extent possible.

Proactive measures are key to preventing the devastating impact ransomware can have on operations and public trust.

<sup>9</sup> [www.trendmicro.com/vinfo/za-en/security/news/cybercrime-and-digital-threats/interceptingimpact-2024-trend-micro-cyber-risk-report](https://www.trendmicro.com/vinfo/za-en/security/news/cybercrime-and-digital-threats/interceptingimpact-2024-trend-micro-cyber-risk-report)

“

Ransomware attacks can potentially drive organisations out of business, so vendors and service providers should be highly motivated to **take all necessary steps to minimise the effects of these attacks across their customer base**”

# Supply chain attack

**A supply chain attack exploits vulnerabilities in third-party vendors or service providers to infiltrate an organisation's network. Attackers leverage the trusted relationships between companies and their suppliers, often inserting malicious code or malware into software updates or tools used across the supply chain.**

A good example of a supply chain attack was US software company SolarWinds in 2020. Hackers infiltrated a technology update from the company. This undetected update was then distributed via SolarWinds to its customers, resulting in the compromise of sensitive networks of thousands of clients, including government agencies and Fortune 500 companies.

The motivation was espionage as the attack was linked to Russia's statesponsored group, Midnight Blizzard (also known as APT29, Cozy Bear, and Nobelium). The goal of the attack was long-term access to sensitive information, particularly within U.S. government agencies and major corporations.

## THE KEY MOTIVATIONS FOR THIS TYPE OF ATTACK ARE:

1

### Espionage:

Gaining access to classified government information, defence strategies, and corporate data

2

### Strategic advantage:

Compromising key U.S. institutions, such as the Treasury and Homeland Security, for geopolitical leverage

3

### Intellectual property theft:

Stealing corporate secrets for economic gain

4

### Disruption:

Though not highly destructive, the breach strained U.S. cybersecurity efforts

## Imperial<sup>™</sup> logistics

COUNTRY	YEAR
South Africa	2022

### EVENT

Imperial Logistics, a key player in South Africa's supply chain and logistics industry, suffered a cyberattack in March 2022. Imperial confirmed that it faced a data breach, which disrupted some of its operations. The attack highlighted the vulnerability of supply chain businesses, as even brief disruptions can affect a wide range of sectors that depend on smooth logistics and distribution.

The pharmaceutical industry has also been a target of supply chain attacks in South Africa, especially during the COVID-19 pandemic, focusing on disrupting distribution chains or stealing sensitive medical data. While specific companies have not been publicly named, reports indicate that attacks on this sector occurred due to its critical importance during the pandemic.

When a software vendor is compromised, a hacker will often be able to gain indirect access to multiple organisations. One breach can affect several companies, leading to data theft, operational disruption, and reputational damage. The NIST Cybersecurity Framework (CSF) core tenets of cybersecurity cover this issue (section 4.2), and it is important to have strong vendor risk management and regularly audit and monitor third-party software. (see sections 5.2 and 5.4).

# Distributed Denial of Service (DDoS) attack

A DDoS attack is a coordinated cyberattack where multiple compromised systems (often part of a botnet) flood a target—such as a server or website—with excessive traffic. This overwhelming traffic overloads the system, causing service disruptions or making it entirely inaccessible to legitimate users. The distributed nature of the attack, coming from numerous sources, makes it challenging to defend against and trace.

## KEY STEPS IN A DDOS ATTACK ARE:

### Botnet control:

Attackers command a network of infected devices (botnet) to generate traffic.

### Traffic Flooding:

The botnet sends large volumes of requests or data packets to overwhelm the target

### Resource exhaustion:

The target's infrastructure is overloaded, exhausting bandwidth, memory, or processing power.

### Service disruption:

As a result, the target becomes slow or completely unavailable to legitimate users.

**These attacks can cause revenue losses and reputational damage and have direct financial costs in the form of mitigation, infrastructure upgrades, and security investments.**

DDoS attacks remain one of the most prevalent and destructive methods used by cybercriminals. Cloudflare reported in its 2024 Global Security Brief on how it uncovered a sustained, highly-coordinated campaign, peaking at an astonishing 201 million requests per second (rps). This highlights the evolving sophistication and scale of threat actors' tactics, underscoring the critical need for robust defence mechanisms.

The GitHub DDoS attack in 2018 was hit one of the largest DDoS attacks ever, peaking at 1.35 Tbps, disrupting services for hours but there was no data breach. The attack was a demonstration of power by the hacker, testing the capabilities of DDoS amplification techniques. These attacks can be mitigated by traffic filtering, rate limiting, and DDoS protections services and form part of evaluating and prioritising data and systems. (see section 5.3)

In 2023, OpIndia, an operation led by the hacktivist group Anonymous, targeted the Indian government and financial websites with DDoS attacks.

The operation disrupted critical online services, including government and financial sectors, by overwhelming websites with traffic, making them inaccessible to the public and severely impacting the operations of targeted entities. Anonymous claimed that the attacks were aimed at protesting the Indian government's handling of social issues, particularly those related to civil liberties, human rights, and the perceived suppression of dissent.

The event is a prominent example of how hacktivism is used as a tool to voice political dissent and protest against government actions through cyberattacks.

It reflects a broader trend where hacktivist groups leverage their technological skills to cause disruption and push for political or social change, targeting governments and critical institutions to challenge policies they disagree with.

# Phishing attack

**A phishing attack is a form of social engineering where cybercriminals impersonate legitimate entities to trick individuals into revealing sensitive information like login credentials or financial data. These attacks typically appear through deceptive emails, messages, or websites. (for responses see section 5.1 on vulnerabilities and 5.2 on employee training)**

Key phishing tactics include email spoofing (fake emails resembling trusted organisations), malicious links/attachments directing users to fraudulent sites or installing malware, or credential theft where someone has gained access to accounts using harvested personal data. Third-party access attacks occur when attackers exploit vulnerabilities in external partners, vendors, or service providers to access an organisation's systems (see supply chain attack, section 3.3).

## ☰ KEY ASPECTS INCLUDE:

### Supply chain weaknesses:

Compromising vendors to breach systems.

### Weak security practices:

Exploiting inadequate cybersecurity among partners.

### Data theft:

Stealing sensitive information or deploying malware.

## PHISHING AND THIRD-PARTY ACCESS

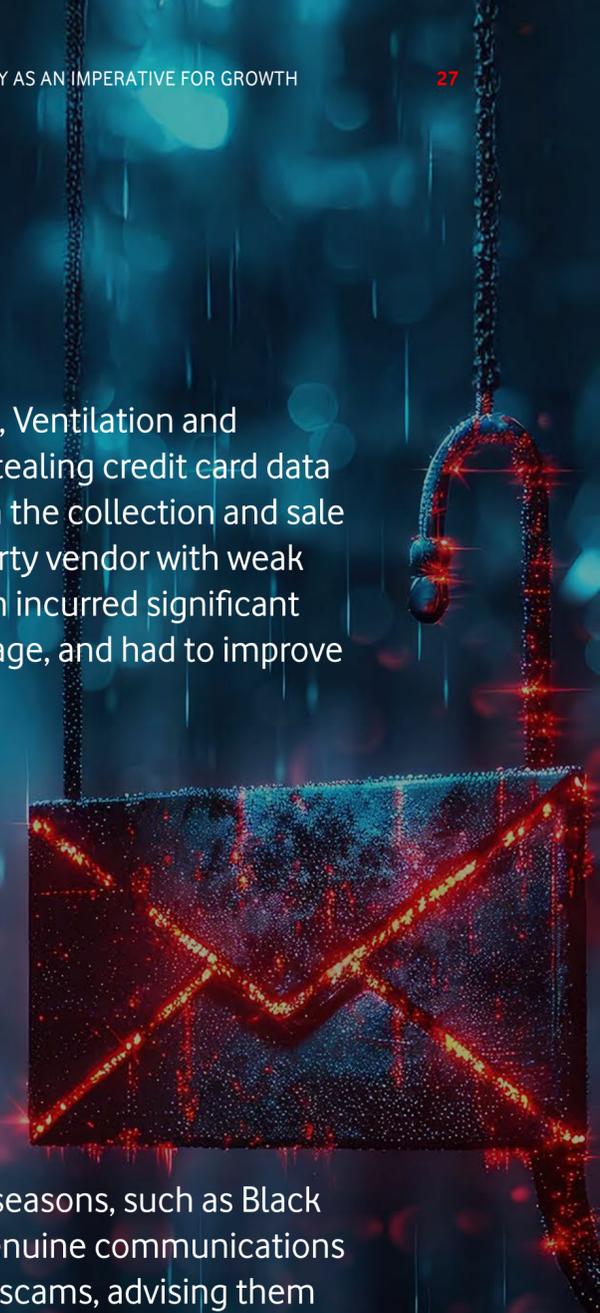
In 2013, hackers used phishing to steal login credentials from a Heating, Ventilation and Airconditioning (HVAC) vendor, gaining access to Target's network and stealing credit card data from over 40 million customers. The hackers were able to profit through the collection and sale of large volumes of stolen credit card data. Attackers targeted a third-party vendor with weak security protocols, infiltrating Target's payment systems. The retail chain incurred significant financial losses, including \$18 million in settlements, reputational damage, and had to improve cybersecurity significantly. The CEO resigned.

The Takealot phishing email scam has been a notable issue, particularly as online shopping increases in popularity in South Africa. These phishing emails purport to be from Takealot, South Africa's largest online retailer, and often claim that users have won gift vouchers or need to update their payment details. The goal is to trick users into providing sensitive information, such as login credentials or payment details, by redirecting them to fraudulent websites that closely resemble Takealot's legitimate platform.

This type of scam has been especially prevalent around busy shopping seasons, such as Black Friday and Cyber Monday, when consumers are more likely to receive genuine communications from retailers. Takealot has warned customers to be vigilant about such scams, advising them not to click on suspicious links and to always verify communications directly on their website.

One interviewee for this report commented that **“online shopping has increased dramatically over the past 3-4 years in South Africa, frequently without sufficient cybersecurity support for many users of these services.”**

These threats underscore the need for strong cybersecurity training, multi-factor authentication, and vendor risk management. (see section 5.4)



# Critical National Infrastructure (CNI) attack

A CNI attack targets essential systems (defined by governments) such as energy, transportation, healthcare, and finance. The goal is to disrupt vital services, leading to significant economic damage, compromising national security, and putting public safety at risk.

## KEY IMPACTS ARE AS FOLLOWS:

### Service disruption:

Halts operations in essential sectors like power grids or water supply, leading to widespread outages.

### Economic losses:

Interruptions in infrastructure lead to financial loss and halted business operations.

### National security risk:

Attacks on defence or government systems can weaken security and expose sensitive data.

### Public safety:

Disruptions in healthcare or emergency services can endanger lives.

→ For more insights into this type of attack please refer to [Critical Infrastructure Protection \(CIP\): Defined And Explained.](#)

## December 2015, a sophisticated cyberattack targeted Ukraine's power grid, leaving 230,000 people without electricity.

Attackers from the Sandworm group used malware to gain control over the SCADA systems managing the grid. The hackers were likely to have been state-sponsored by Russia, the goal being to destabilise Ukraine's infrastructure amidst political tensions. This was the first confirmed cyberattack to cause a power blackout, highlighting the vulnerability of critical infrastructure globally.

In July 2021, Transnet, South Africa's state-owned entity responsible for freight, rail, and port management, was hit by a major cyberattack (see section 3.3). The incident was so severe that Transnet was forced to declare a force majeure at several ports, meaning they could not fulfil their contractual obligations due to circumstances beyond their control. This declaration effectively paused the operations of vital shipping routes and impacted global trade for several days, especially as cargo movements were halted.

The Transnet cyberattack highlighted South Africa's vulnerability in protecting its critical transportation infrastructure from cyber threats. The logistics and supply chain disruption not only affected the country's economy but also underscored the risks that cyberattacks pose to national and international trade.

The attack was part of a broader wave of ransomware incidents targeting critical infrastructure globally, underlining the need for enhanced cybersecurity measures across vital sectors such as transportation, logistics, and energy.

Governments and other organisations combat these risks with strong cybersecurity measures, redundancy plans, and collaboration with agencies like CISA (Cybersecurity and Infrastructure Security Agency) in the US.

# Next-generation threats: Navigating the future of digital defence

**As technology continues to evolve, so do the tactics of cybercriminals. The rise of next-generation cybersecurity threats introduces more complex challenges that require advanced defence strategies.**

From AI-powered attacks to quantum computing exploits, the digital landscape is becoming increasingly treacherous. These emerging threats target critical infrastructure, leverage 5G networks, and exploit the vulnerabilities of autonomous systems, making traditional security measures insufficient. To stay ahead, organisations must adopt forward-looking strategies and innovative solutions to mitigate these evolving risks. Understanding these next-gen threats is the first step in fortifying your digital defences for the future. These next-generation cybersecurity threats are expected to shape the future landscape.



## ARTIFICIAL INTELLIGENCE-POWERED ATTACKS

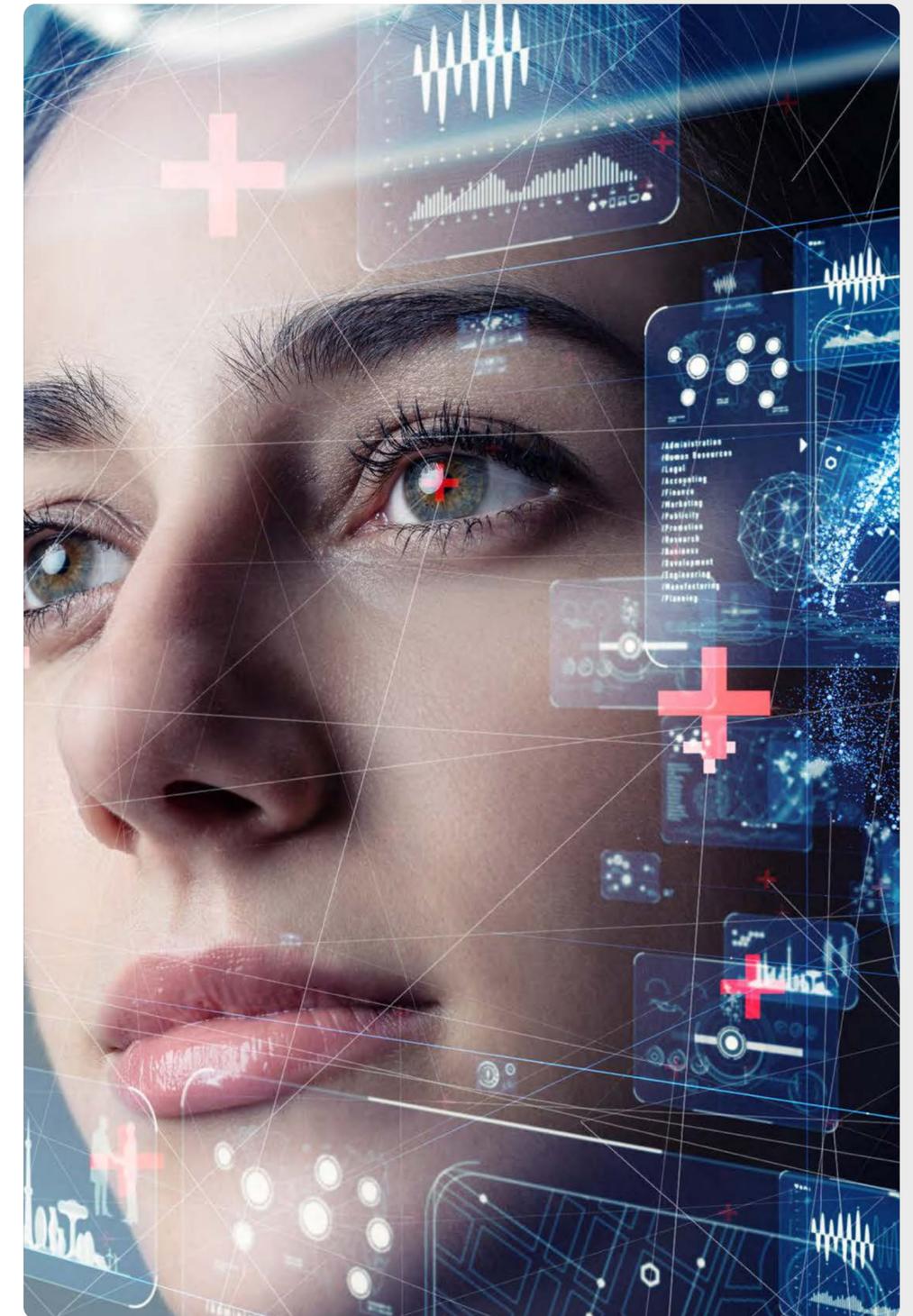
Cybercriminals are increasingly exploring and testing AI, including large language models (LLMs), to enhance their attack strategies and circumvent security measures, as noted here by Microsoft. Organisations must focus on strengthening security controls and deploying advanced monitoring systems that proactively detect and prevent AI-enhanced threats. Staying ahead of these tactics requires ongoing investment in AI-driven cybersecurity solutions and threat intelligence.

Attackers use AI to enhance and automate cyberattacks, making phishing, malware, and other tactics more sophisticated and harder to detect. AI-driven attacks can quickly adapt to defensive measures, resulting in faster,

more widespread breaches that can bypass traditional cybersecurity defences. Organisations employ AI-driven security tools that can detect and respond to anomalies in real-time.

Voice mimicry using AI-powered tools has become a sophisticated method of cybercrime. A notable case occurred when criminals used voice-generating AI to imitate the voice of the CEO of a UK-based energy company. The AI replicated the CEO's voice pattern, tone, and accent convincingly enough to deceive the company's finance team into thinking they were speaking with the actual CEO.

The fraudsters used this imitation to request an urgent wire transfer, presenting the situation as a business emergency. Believing the request



was genuine, the finance department transferred hundreds of thousands of dollars to the fraudulent account provided by the criminals. This scam highlights the dangers of AI-based deepfakes in the realm of social engineering attacks, where convincing digital forgeries can be used to manipulate individuals or systems into making costly mistakes.

Recognised globally, this case serves as a warning for organisations to implement multi-factor authentication and robust verification protocols for financial transactions, particularly when such requests appear urgent or out of the ordinary. It also demonstrates the emerging risks associated with AI technology, as its misuse can lead to sophisticated and convincing impersonation, potentially causing significant financial and reputational damage.



### QUANTUM COMPUTING THREATS

Quantum computers could break encryption algorithms currently protecting sensitive data, exposing organisations to data breaches. Current encryption methods like RSA (Rivet-Shamir-Adleman) or ECC (Elliptic Curve Cryptography) could become obsolete, allowing attackers to decrypt sensitive communications and steal confidential data. Organisations need to monitor advances in post-quantum cryptography to prepare for future quantum challenges.

In South Africa, there is increasing awareness of these potential vulnerabilities. Organisations operating in critical sectors such as banking, energy, and telecommunications are starting to explore quantum-resistant cryptography to safeguard against future threats. Additionally, the rapid digital transformation across industries like finance and telecommunications requires businesses to remain alert to advances in quantum computing technology and to implement proactive measures, such as quantum-safe encryption, to protect sensitive data.

As these developments progress, South African organisations should consider quantum-readiness strategies, which include conducting risk assessments, updating their cryptographic infrastructure, and preparing for post-quantum cryptographic standards to ensure long-term data security.



### DEEPPAKE-BASED SOCIAL ENGINEERING

Deepfakes, including using AI to mimic a person's voice (see above, artificial intelligence-powered attacks), can be used to impersonate high-profile individuals, tricking victims into providing sensitive information or authorising fraudulent transactions. Deepfake attacks can lead to significant financial losses, data breaches, and reputational damage due to fraudulent activities. These can be defended against using verification methods like multi-factor authentication for sensitive transactions and educating employees to recognise potential deepfake content and adopt cautious behaviour in digital communications. (see section 5.2)

There has been a dramatic increase in deepfake fraud reported in 2023 and 2024. **There has been a 1,200% surge in such cases across South Africa**, with criminals using AI-generated voices and videos to impersonate high-profile individuals. This technology is becoming a significant threat, especially in the financial sector, where it has been used to deceive people into authorising fraudulent transactions by mimicking the voices of executives or trusted associates.

To defend against such attacks, verification methods should be deployed such as multi-factor authentication (MFA) for sensitive transactions, as well as educating employees to be vigilant and recognise the potential dangers of deepfake content.



## AUTONOMOUS SYSTEMS EXPLOITS

Autonomous systems, such as drones and self-driving cars, are vulnerable to exploits targeting their AI, leading to potential control and safety risks. Exploits in autonomous systems can result in physical harm, operational disruptions, and compromised control over essential technologies. To mitigate these risks, South African businesses are encouraged to deploy advanced cybersecurity measures, including drone detection systems and isolating critical networks from less secure external connections (see section 5.6). This is crucial in industries like mining and energy, where drones are widely used, but could also pose significant threats if compromised. These proactive approaches, along with continuous monitoring, can help maintain control over essential autonomous technologies and prevent potential breaches or operational failures.

In South Africa, the growing use of drones in various sectors has also increased the risks associated with autonomous systems. For instance, drones are being widely adopted for security, surveillance, and even by state-owned enterprises like Transnet and PRASA to protect critical infrastructure. However, attackers can potentially take control of drones or use them to create fake Wi-Fi hotspots to access sensitive corporate networks, conduct surveillance, or disrupt operations. Other vulnerabilities could allow malicious actors to intercept sensitive data or cause physical harm by manipulating the flight path of drones used for security.

These emerging threats increase the risk of data breaches, operational disruptions, and physical harm. To mitigate risks, organisations must adopt advanced tools such as AI-driven defences, quantum-resistant encryption, and proactive models. Ensuring continuous monitoring, robust backups, and collaboration on infrastructure protection is essential for staying ahead of evolving cyber risks. This forward-looking approach is key to maintaining resilience in the face of sophisticated cyber threats.

These proactive approaches, along with continuous monitoring, can help maintain control over essential autonomous technologies and prevent potential breaches or operational failures.



## LEVERAGING 5G NETWORKS

The rollout of 5G expands the attack surface, especially with the use of IoT devices, potentially allowing attackers to exploit weak security in connected systems. Attacks on 5G networks can lead to widespread breaches, data theft, and service disruptions, particularly for IoT devices. There is a need for endpoint security where security for all devices connected to the 5G network are strengthened and specialised IoT security measures are implemented.



# Understanding what cybersecurity affects

04



# The scope of cybersecurity in an organisation and beyond

In most companies, cybersecurity is far from a single discipline and although almost everyone who thinks about it knows it is important, there are common issues that undermine its successful implementation. Those interviewed for this paper identified staff shortages, support for new digital projects (e.g. cloud migration), and insider threats as key issues.

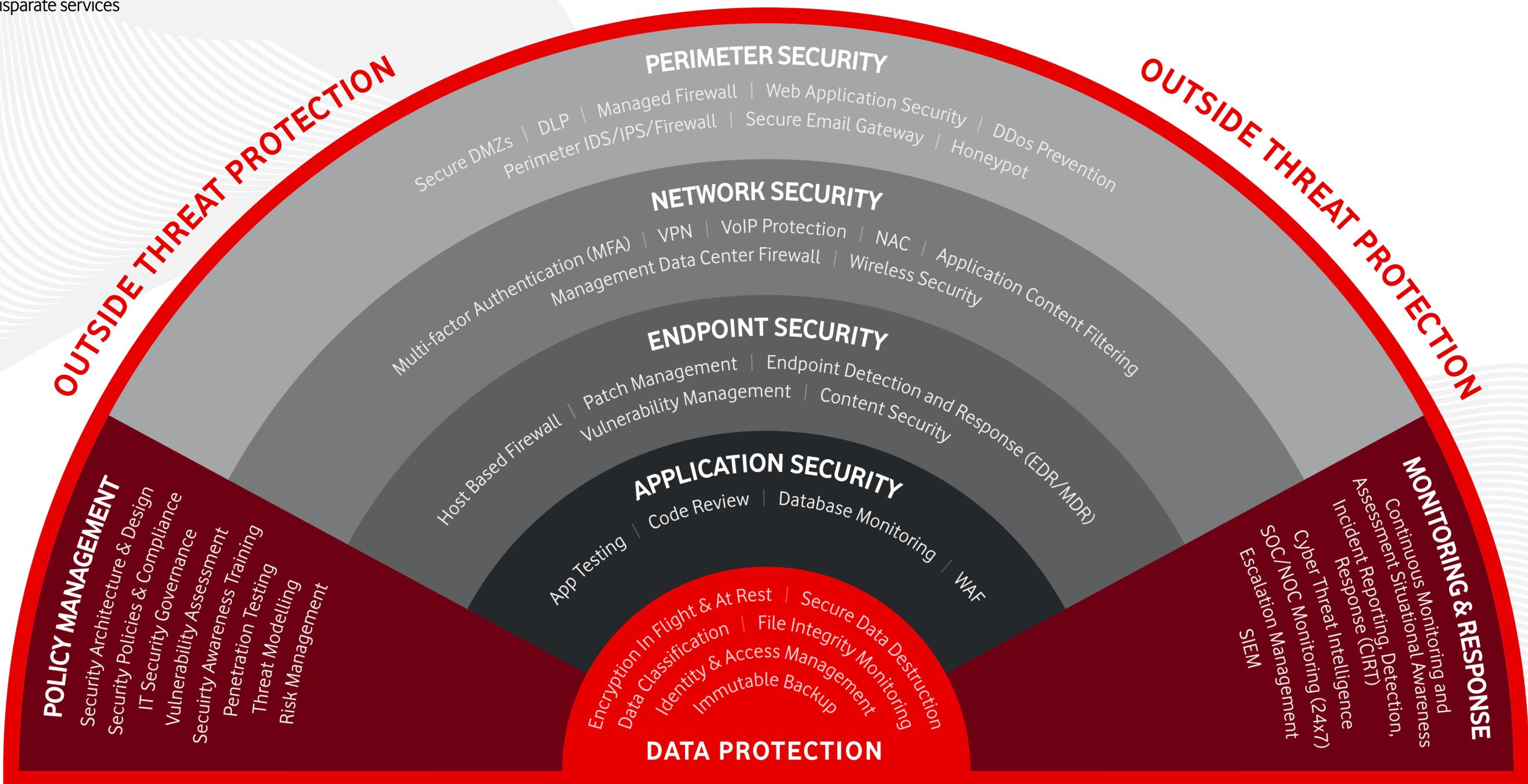
This is backed up by Omdia's Cybersecurity Decision Maker survey, which highlighted the workforce shortage, digital transformation projects, employee training, and budget top amongst the challenges faced<sup>10</sup>. As one regional company executive noted: **"Global salary competition is a challenge for attracting and retaining talent in Africa, as workers may earn higher salaries in other regions while living in Africa."**

The graphic overleaf illustrates the vast scope and complexity of the cybersecurity technology landscape. Vendors and service providers frequently deliver comprehensive technology and services focusing on one or a few of the capabilities below.

<sup>10</sup> Omdia Cybersecurity Decision Maker Survey 2024, n=964

# DEFENCE-IN DEPTH

We bring consolidated visibility and integration of disparate services





Cybercriminals only need to exploit a single vulnerability to breach an organisation's defences, hence the need for "defence in depth" – multiple layers of cybersecurity technology, alongside people and process, to protect and defend the organisation. As this complexity continues to grow, more vendors of cybersecurity technology will partner with service providers to support the "defence in depth" approach<sup>11</sup>. Canals reports that today, 90% of cybersecurity spending is sold through and with partners. Furthermore, Canals expects that this number is higher in Africa, because of lack of in-country local resource from the vendor.

As seen in 3.3 above, it's critical that cybersecurity measures extend beyond internal operations to encompass the entire supply chain. Ensuring third-party partners adhere to the same rigorous legal and security standards is not just a best practice—it's essential for safeguarding the integrity of the entire ecosystem. One executive in a major regional company emphasised this point: **"A major challenge for us is managing security risks associated with third-party vendors. Breaches in third-party systems often have a cascading effect, impacting our own security. We have initiated programs to educate and work closely with third parties to improve their security measures."**

<sup>11</sup> Canals research notes that 81% of cybersecurity channel partners expect growth in cybersecurity business in 2024, compared to 2023, Sep 2024, n=246

# The core tenets of cybersecurity

The global rise in cyber threats has elevated the need for structured and proactive cybersecurity approaches, and the likes of the NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) have emerged as guiding tools.

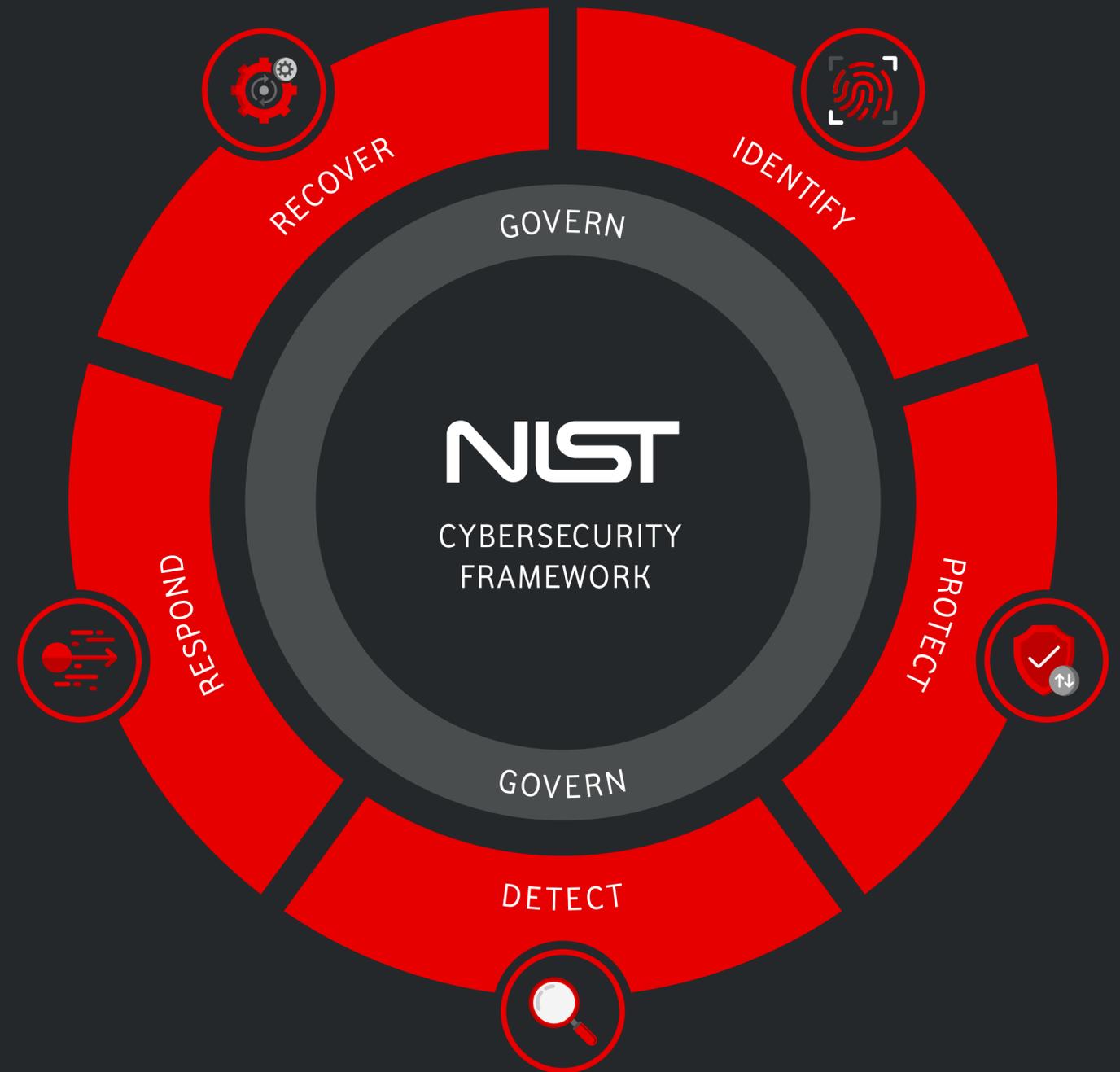
Originating in the USA, this framework has gained worldwide adoption, including in South Africa, due to its comprehensive approach to security governance. One interviewee commented that **“the NIST CSF is the de facto standard – everyone is using it”**.

The NIST CSF revolves around five key functions— **identify, protect, detect, respond, and recover**—offering a roadmap for organisations to navigate the complexities of cybersecurity. It helps organisations not only identify potential threats but also implement robust mechanisms to protect their systems, detect intrusions, respond effectively to incidents, and recover swiftly from attacks.

Similarly, ISO 27001, the international standard for information security and privacy protection, is widely adopted.

Vendors, their partners, and service providers are wellversed in various frameworks and assist customer organisations in adopting cybersecurity technologies and services aligned with these frameworks.

By integrating elements from these frameworks, organisations can significantly enhance their security posture and adopt a comprehensive approach to risk management. This also results in them being better equipped to embed cybersecurity into their culture and day-to-day practices. This holistic approach strengthens trust with stakeholders, ensures regulatory compliance, and provides a competitive advantage in the increasingly digital global marketplace.



Source : <https://www.nist.gov/cyberframework>

## HOW ORGANISATIONS CAN START USING THE NIST CYBERSECURITY FRAMEWORK

The NIST CSF provides a structured approach for organisations to enhance their cybersecurity posture. To begin using this framework, organisations can follow these steps:



## CHALLENGES FOR ORGANISATIONS WITH LIMITED CYBERSECURITY EXPERTISE OR RESOURCES

For businesses with limited cybersecurity expertise or resources, implementing the NIST CSF can be more challenging. Resource constraints mean that certain categories of organisation like small and medium-sized businesses (SMBs) may lack the budget for dedicated cybersecurity staff, technology, or external consultants. One interviewee for this report commented that **“when it comes to cybersecurity, the SMB sector has fewer resources, minimal budgets, putting them at greater risk”**.

One company’s cybersecurity executive, who deals with organisations of this type noted: **“Small businesses often struggle with cybersecurity due to limited resources and knowledge. They might have one IT person juggling multiple roles. Large customers typically conduct detailed security assessments and request certifications like ISO. Smaller customers rarely ask cybersecurity questions, focusing more on cost and contracts.”**

Those lacking resources may need to start with the most critical functions, such as Identify (knowing their assets and risks) and Protect (implementing basic defences like firewalls, antivirus software, and encryption). The key differences for this category of organisations are:

- **Simplified implementation:**  
SMBs can focus on the most relevant and feasible parts of the framework. For instance, they can start with simplified versions of the NIST recommendations, such as ensuring proper access control and endpoint protection, without fully adopting every part of the framework.
- **Use of managed services:**  
Organisations with limited expertise may benefit from outsourcing cybersecurity functions to Managed Security Service Providers (MSSPs) who can handle monitoring, threat detection, and incident response on their behalf, supporting industry standards like the NIST CSF.
- **Gradual adoption:**  
Businesses with fewer resources can adopt the NIST framework incrementally. They can focus on implementing basic cybersecurity hygiene, such as regular software updates, secure password policies, and employee training, and gradually build up to more advanced protections like automated monitoring and incident response.

In summary, while large organisations may have the resources to adopt the NIST CSF comprehensively, smaller businesses can still benefit by focusing on essential practices and gradually expanding their cybersecurity capabilities. Outsourcing and prioritising critical areas help ensure security measures are manageable and effective. (see section 5.7 on not going it alone).



# Cybersecurity as the backbone of resilient digital tenets

The relationship between cybersecurity, resilience, and digital innovation is vital for organisations looking to thrive in today's digital economy. As one cybersecurity expert interviewed said: **“Developers are often pressured to prioritise speed over secure coding practices, leading to vulnerabilities.”**

Cybersecurity serves as a foundational element that allows companies to innovate with confidence, ensuring that new digital products and services are resilient against evolving cyber threats.

South African companies like Discovery, Standard Bank, Nedbank, and Vodacom have successfully embedded cybersecurity into their innovation strategies. These organisations have demonstrated that a proactive approach to security not only safeguards their operations but also drives digital innovation and builds resilience against cyber threats.



DISCOVERY



## Securing digital healthcare platforms

Discovery, one of South Africa's largest health insurance companies, has embraced digital innovation through its Vitality program and various digital healthcare platforms. Recognising the sensitive nature of healthcare data, Discovery has embedded robust cybersecurity measures to safeguard personal and health-related information. Through initiatives such as encryption, secure authentication, and continuous monitoring of cyber threats, Discovery ensures that its innovative digital health offerings are resilient to potential breaches.

By prioritising cybersecurity in the development of these platforms, Discovery has been able to innovate confidently, offering secure health management tools that maintain customer trust.

## NEDBANK



### Cybersecurity in data analytics innovation

Nedbank, another major South African bank, has embedded cybersecurity into its data analytics-driven innovation. Nedbank uses big data analytics to drive insights and improve customer services, but this also introduces new cybersecurity risks. The bank has adopted a proactive stance on cybersecurity by implementing encryption, access controls, and secure data storage systems to protect its customers' information. This resilience has allowed Nedbank to leverage advanced technologies such as AI and machine learning while maintaining a strong defence against evolving cyber threats.

## VODACOM



### Embedding cybersecurity in IoT and connectivity innovations

As a leading telecom operator in South Africa, Vodacom has heavily invested in Internet of Things (IoT) solutions, expanding into areas like smart cities and connected devices. To manage the cybersecurity risks associated with IoT, Vodacom has implemented strong security protocols that ensure devices and networks are protected from unauthorised access. By embedding cybersecurity into its IoT innovations, Vodacom provides secure connectivity solutions that meet both customer needs and regulatory standards.

Leading global companies are also advancing innovation while reinforcing their resilience against increasing cyber threats.

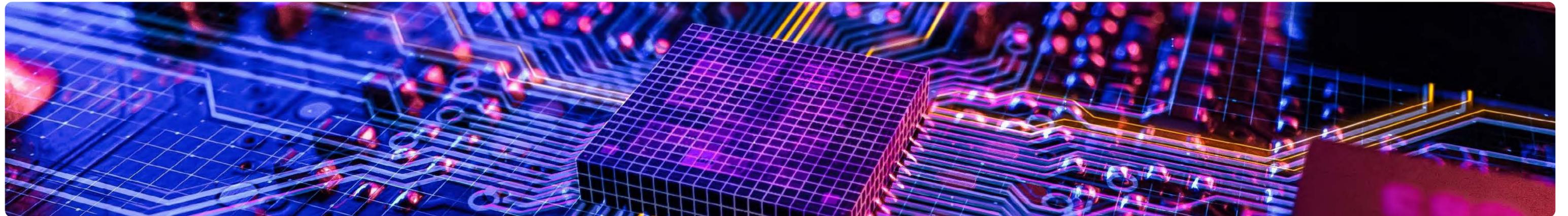
## NESTLÉ



### Cybersecurity as a growth enabler

Nestlé, as part of its digital transformation, has embedded cybersecurity into its business processes to ensure that innovation can flourish without exposing the company to undue risk. By building a cybersecurity-first culture and employing advanced monitoring systems, Nestlé ensures its global supply chain operations are secure. This has enabled the company to adopt technologies like blockchain to improve transparency and efficiency in its supply chain.

The integration of cybersecurity into Nestlé's innovation framework has enabled it to maintain resilience while experimenting with advanced technologies, ensuring that cyber risks are minimised during the digital transformation process.



BMW

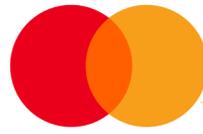


## Safeguarding connected vehicles

The automotive industry is a hub of digital innovation, especially with the rise of connected vehicles. BMW has successfully integrated cybersecurity into its innovation lifecycle to ensure its vehicles remain protected from cyber threats. Through a combination of encryption, authentication mechanisms, and secure software updates, BMW safeguards its autonomous driving systems and vehicle-to-everything (V2X) communication technology.

BMW's approach not only ensures that its vehicles are resilient against hacking attempts but also allows it to continue innovating in the areas of autonomous driving and smart vehicle ecosystems.

MASTERCARD



## Building trust in digital payments

Mastercard has placed cybersecurity at the core of its digital innovation strategy to build consumer trust and enable digital payments globally. By embedding advanced security technologies like AI and machine learning into its payment systems, Mastercard ensures transactions are secure while fostering innovation in digital banking and e-commerce. The company uses its Cyber Resilience Centre to monitor and protect its vast infrastructure, ensuring that new digital payment innovations are resilient against cyber threats.

Mastercard's proactive cybersecurity stance not only enhances customer trust but also enables the company to continuously innovate in areas like contactless payments and digital wallets, knowing that its systems are secure.

Cybersecurity plays a critical role in driving innovation by safeguarding digital infrastructure from threats. By embedding cybersecurity from the start, companies can innovate confidently without fear of disruption. Resilience ensures that businesses can quickly recover from cyber incidents, maintaining operational continuity. When cybersecurity is viewed as a strategic enabler, it enhances trust, supports growth, and ensures innovations remain secure and scalable.

By viewing cybersecurity as a strategic enabler rather than a cost, organisations can ensure that their innovations are secure, resilient, and scalable for the future

STANDARD BANK



## Cybersecurity as an enabler of FinTech innovation

As one of South Africa's largest financial institutions, Standard Bank has made significant strides in digital innovation, particularly in the area of mobile and online banking. To ensure the safety of its clients' financial data, Standard Bank integrates advanced cybersecurity measures, including multi-factor authentication, biometric verification, and AI-powered fraud detection. This focus on security allows the bank to continuously innovate with digital payment systems and mobile banking solutions while ensuring resilience against cyberattacks. This proactive approach enables Standard Bank to remain a leader in financial technology (FinTech), confident that its innovations are built on secure foundations.

# Cybersecurity as a business enabler: Measuring ROI and long-term value

**In the modern digital economy, cybersecurity has evolved from a defensive necessity into a strategic business enabler. Once viewed as a cost centre, cybersecurity is now recognised for its capacity to protect business continuity, drive operational efficiency, and foster innovation. By preventing costly breaches, building customer trust, and ensuring compliance with regulatory standards, strong cybersecurity measures directly contribute to an organisation's bottom line.**

This section explores how proactive investment in cybersecurity not only reduces risks but also delivers tangible financial benefits. From avoiding significant financial losses due to breaches and operational disruptions to enhancing customer loyalty and unlocking new digital opportunities, robust cybersecurity is integral to long-term growth and resilience.

## COST SAVINGS FROM AVOIDING CYBER BREACHES

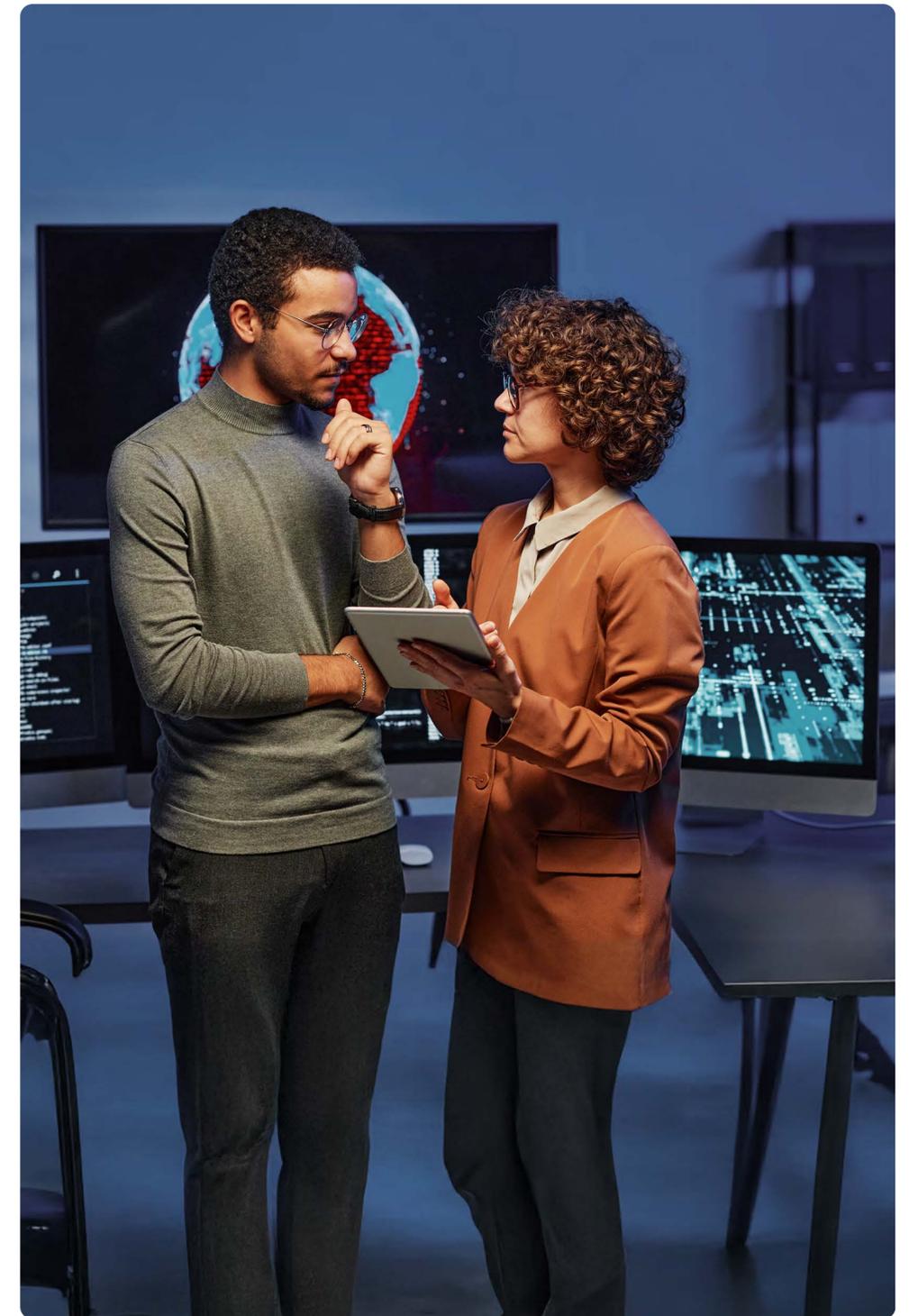
Data breaches are increasingly expensive, with the global average cost of a breach reaching \$4.88 million in 2024, as referenced earlier in this paper from IBM's Cost of a Data Breach Report. Omdia research also highlights that globally, for organisations with fewer than 1,000 employees, 80% had suffered a breach costing up to US\$50,000<sup>12</sup>. The same survey notes that 34% of that same group of organisations had suffered a breach event costing over US\$500,000. Avoiding these costs through preventive cybersecurity measures is a clear financial benefit.

Breaches often cause downtime, which can cripple business operations and lead to revenue loss. Investing in security systems that prevent such incidents helps businesses avoid these costly disruptions.

Cybersecurity incidents can severely damage customer trust and lead to lost business. A strong security posture fosters customer confidence, especially when handling sensitive data. This leads to higher customer retention rates and helps maintain a company's reputation. Avoiding a breach protects a company's brand, preventing the long-term financial damage that often follows a high-profile cyberattack.

In the public sector, reputation is tied to public trust rather than customer loyalty. When a government entity or public service experiences a cyberattack, it risks eroding the trust that citizens place in its ability to protect sensitive information, such as healthcare or personal identity data. For instance, a breach in a national health system could lead to public fear over medical records being exposed, creating a ripple effect of distrust across various governmental services.

Public sector organisations often face higher levels of scrutiny than private businesses. When cybersecurity incidents occur, public entities are expected to manage the crisis transparently and swiftly, often with challenging budgets. Mishandling a breach can lead to reputational damage not only for the department involved but for the broader government as well.



<sup>12</sup> Omdia Cybersecurity Decision-Maker Survey, 2024 n=198



Although public sector entities may not have traditional "brands," their reputational capital lies in their perceived competence, reliability, and security. For government agencies, avoiding breaches means protecting this "brand" of public trust. Failing to do so can lead to a loss of confidence in services, voter dissatisfaction, and political consequences.

While public entities don't compete for market share like private companies, they do rely on maintaining their reputational value to ensure uninterrupted funding, public cooperation, and efficient operations. A cybersecurity breach could lead to higher costs in restoring systems, facing legal challenges, or managing public backlash, which can divert resources from other essential services. Often, public sector organisations have not kept up technologically, according to one cyber expert familiar with their IT operations:

"Public sector challenges often involve legacy systems and slow migration to modern systems."

Strong cybersecurity supports compliance with regulations such as POPIA and GDPR, avoiding fines that can reach up to 4% of global turnover for GDPR. This protects businesses from legal penalties and potential lawsuits

Enterprise purchasing of insurance policies against cyber-based risks and various cybersecurity-related worst-case scenarios has become standard operating procedure for many organisations in South Africa and beyond. Insurance providers are increasingly active in the provision of this insurance, requesting evidence of cybersecurity investments. Interviewees noted that

"Cybersecurity investments can lead to lower insurance premiums as insurers reward companies that demonstrate reduced risk through robust security measures".

By reducing the frequency of security incidents and breaches, cybersecurity investments enhance overall productivity, preventing costly downtime and ensuring smoother business operations. Secure systems facilitate new digital initiatives, such as cloud migration or IoT adoption, without the added risk of security breaches.

Cybersecurity is no longer a line-item expense to manage; it's a crucial strategic investment that directly impacts an organisation's financial health. Robust cybersecurity measures protect revenue streams, maintain operational stability, and fortify organisations' reputations — key drivers for long-term success

A cybersecurity breach can halt operations, incur significant financial losses, and erode customer trust, all of which threaten business continuity and growth. On the other hand, investing in comprehensive security not only mitigates these risks but also improves ROI by preventing costly incidents, maintaining customer confidence, and positioning the company as a reliable market leader.

In today's competitive landscape, cybersecurity is essential for growth and resilience, ensuring that organisations remain agile, innovative, and trusted while driving both immediate and long-term financial returns.

# What organisations need to do

Whether an organisation's security function consists of a large team or just one person, cybersecurity must be considered and addressed. Under eight different headings, this section provides recommendations across an organisation.

# CS



# Know your vulnerabilities

Ignoring cybersecurity vulnerabilities is like leaving doors and windows open, inviting opportunistic attacks. To protect your organisation, it's essential to vigilantly identify and address security gaps before they can be exploited. Regularly scanning for vulnerabilities and promptly patching systems is vital in ensuring that attackers don't find weak points to exploit.

This is not a task for IT alone—collaboration between IT and cybersecurity teams is critical to ensure vulnerabilities are patched quickly and prioritised based on their risk level and potential impact. According to the 2024 Trend Micro Cyber Risk Report, the African region patches vulnerabilities at 28 days<sup>13</sup> - this means that there are 28 days for attackers to exploit those vulnerabilities.

Cybercriminals often target backup systems, knowing that a compromised backup can cripple an organisation's recovery efforts. As such, implementing robust data and system backup strategies is essential. Backups must be protected against ransomware attacks to ensure they remain secure and available when needed most.

Another common attack vector is credential theft. This method allows hackers to bypass traditional security measures and gain unauthorised access to sensitive data. To mitigate this risk, organisations must implement effective user lifecycle management, ensuring that access credentials are monitored, controlled, and protected. Additionally, deploying multi-factor authentication (MFA)—which uses multiple methods to verify identity, such as a user ID, password, and biometric data—adds a crucial layer of security, making credential theft much more difficult for attackers.

Strengthening these defences requires ongoing engagement with cybersecurity experts and leveraging external resources to ensure your organisation's overall security posture is continuously improving. Interviewee comments included that **“it is difficult to attract and retain cyber talent, so partnership with experts is essential to manage security posture”**.

<sup>13</sup> [www.trendmicro.com/vinfo/za-en/security/news/cybercrime-and-digital-threats/intercepting-impact-2024-trend-micro-cyber-risk-report](https://www.trendmicro.com/vinfo/za-en/security/news/cybercrime-and-digital-threats/intercepting-impact-2024-trend-micro-cyber-risk-report)



## ACTIONS

**1**  
**Conduct regular vulnerability scans**

Frequently scan for vulnerabilities across systems, networks, and applications to identify potential security gaps early.

**2**  
**Patch systems promptly**

Prioritise and quickly patch identified vulnerabilities based on their risk level to prevent exploitation by attackers.

**3**  
**Strengthen backup systems**

Implement robust data backup strategies and protect backups from ransomware attacks, ensuring they are secure and available for recovery when needed.

**1****2****3****4**  
**Implement Multi-Factor Authentication (MFA)**

Use MFA to add extra layers of security, making it harder for attackers to gain unauthorised access through credential theft.

**5**  
**Deploy effective user lifecycle management**

Continuously monitor and control access credentials, ensuring only authorised individuals have the necessary permissions. People leaving the organisation are a clear target for revoking credentials.

**6**  
**Engage cybersecurity experts**

Regularly consult with external cybersecurity experts and leverage external resources to enhance your organisation's security posture and defence mechanisms.

**4****5****6**

Taking these steps will help maintain resilience and prevent operational disruptions.



# Review your cybersecurity controls: People, process and technology

**Effective cybersecurity controls are built on three key pillars: people, process, and technology. Some organisations have carefully designed these controls, while others have developed them by default over time.**

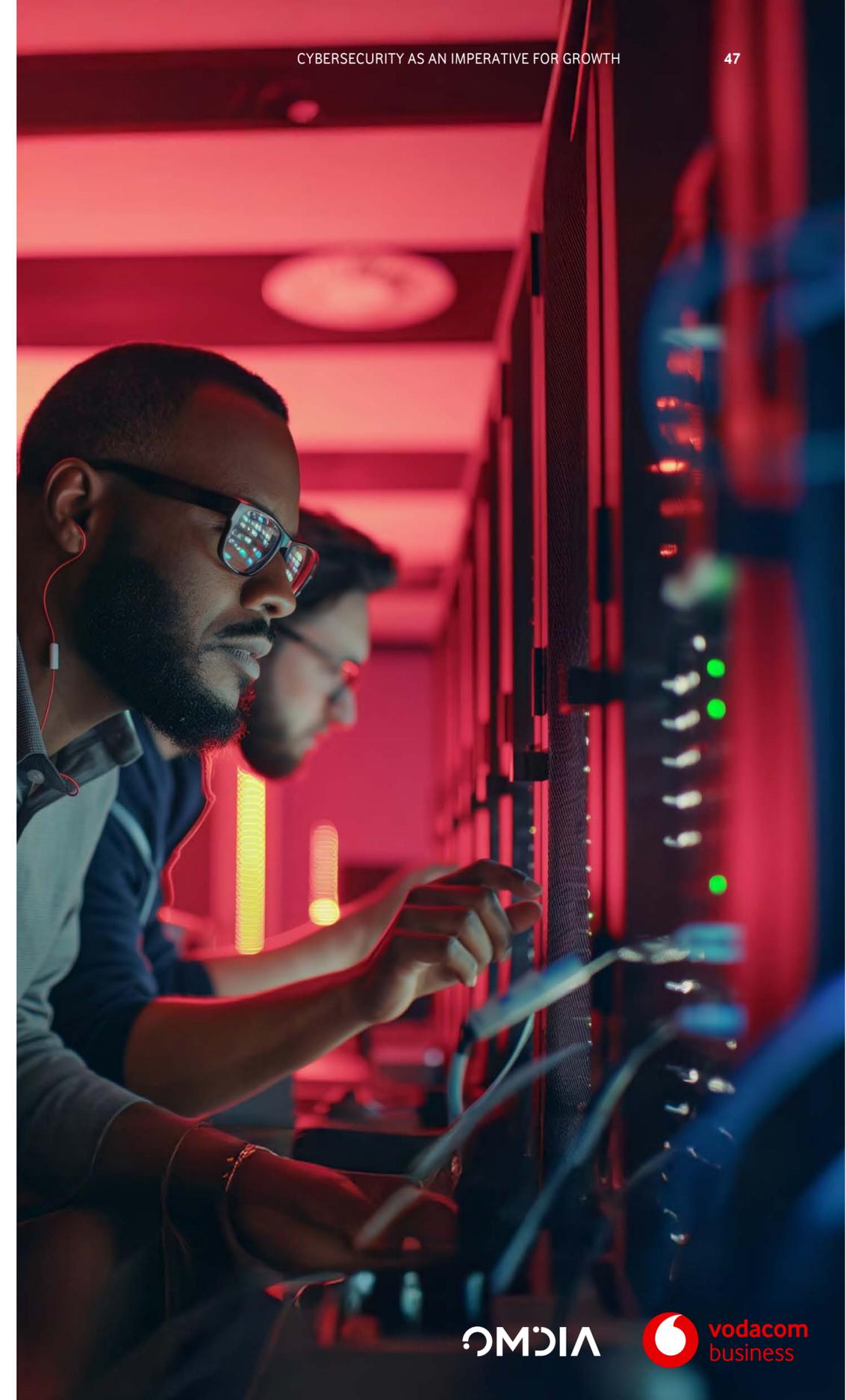
Regardless of the starting point, the journey to robust cybersecurity begins with a clear assessment of where you stand. Interviewees for this report consistently recommend conducting a cybersecurity maturity assessment, particularly for organisations at the beginning of their cybersecurity journey. Interviewees also commented that an assessment is valuable for those organisations unsure about their security posture. Such an assessment provides a roadmap for identifying gaps and creating a strategic plan to strengthen defences.

Among the three pillars, the technological component offers the greatest opportunity for improvement. Automation and artificial intelligence (AI) tools are increasingly used to support human teams to monitor networks, detect anomalies, and identify potential vulnerabilities. AI has become an invaluable asset in cybersecurity, augmenting the workforce and enabling faster, more precise threat detection. Another critical advancement is network segmentation—the practice of isolating key assets to limit the spread of malware and ransomware, thus reducing the risk of a widespread attack.

In addition to adopting cutting-edge technologies, organisations should review the existing software tools they are already using. Many of these tools have integrated security features that are often underutilised. By leveraging these built-in capabilities, organisations can further enhance their defence strategies without significant additional investment. Collaboration with legal teams is also essential to ensure that cybersecurity measures meet regulatory requirements, while tailored controls are implemented to address specific risks faced by the organisation.

Finally, cybersecurity controls must extend beyond the organisation's internal operations to include the supply chain. As businesses grow and evolve, the target operating model for cybersecurity should mature accordingly, ensuring that external partners and suppliers adhere to the same rigorous standards as the organisation itself.

Taking a strategic, integrated approach to cybersecurity controls—focused on people, process, and technology—ensures that your organisation is not only compliant but also resilient. In a world where threats are evolving rapidly, proactive planning and technological innovation are key to staying ahead.



## ACTIONS

**1 Conduct a cybersecurity maturity assessment**

Start by evaluating your current cybersecurity status or updating any existing assessment. This provides a roadmap for identifying gaps and planning improvements.

1

**2 Leverage automation and AI tools**

Invest in AI-driven tools to monitor networks, detect anomalies, and identify vulnerabilities. This improves threat detection speed and accuracy.

2

**3 Implement network segmentation**

Isolate critical assets to limit malware or ransomware spread and reduce overall risk.

3

**4 Maximise existing security features**

Review and fully utilise security features in your current software tools to enhance protection without significant additional costs.

4

**5 Ensure regulatory compliance**

Collaborate with legal teams to align cybersecurity measures with regulatory requirements, ensuring compliance and minimising legal risks.

5

**6 Extend security to the supply chain**

Ensure your external partners and suppliers follow the same rigorous security standards to avoid vulnerabilities across the entire ecosystem.

6

**7 Integrate people, process, and technology**

Develop cybersecurity strategies that integrate human oversight, structured processes, and cutting-edge technology to build a resilient defence system.

7

**By integrating these steps, your organisation will improve both compliance and resilience in the face of evolving cyber threats.**



# Evaluate and prioritise your data and systems

In today's digital economy, cybersecurity must be a top consideration in the development of every digital product and service. Security teams and developers need to collaborate closely, ensuring that application code is not only functional but secure.

This involves proactively identifying potential vulnerabilities, prioritising them based on their severity, and implementing effective remediation strategies. When security is baked into the development process, the resulting digital products have fewer vulnerabilities, significantly reducing risk for the organisation and its customers.

The benefits of secure code go beyond protection—it enables greater confidence in digital innovation. Products developed with cybersecurity in mind are less likely to expose the organisation to the threats that can disrupt operations, compromise data, or damage customer trust. The reduced risk that comes from secure development practices allows organisations to scale and innovate without fear of unexpected security breaches.

However, not all data and digital systems are equal in their importance. Mission-critical assets, which are those essential to an organisation's operational continuity, must be identified and prioritised for protection. If the unavailability or compromise of a particular system or dataset would cause significant disruption, it demands the highest level of security. By focusing cybersecurity efforts on these critical areas, organisations can ensure that they remain resilient, even in the face of potential threats. One interviewee commented that **“it is essential to understand the organisation’s ‘crown jewels’, determining what could happen if these were compromised through a cyberattack”**.

Prioritising security in digital development is not just about protecting data—it's about building a future-proof operation. Organisations that integrate cybersecurity into the DNA of their digital products not only reduce their exposure to risks but also position themselves to operate confidently in an increasingly connected and competitive world.

**ACTIONS**

**1 Identify mission-critical assets**

Begin by assessing your data and systems to determine which are essential to operational continuity. Prioritise securing these assets with the highest level of protection.

**2 Collaborate between security and development teams**

Ensure close collaboration between your cybersecurity and development teams. Build security into the application development process to proactively identify vulnerabilities and reduce risks.

**3 Implement secure code practices**

Integrate security into the software development lifecycle (SDLC) by enforcing secure coding practices. This reduces vulnerabilities in digital products and helps avoid costly breaches.

**4 Focus on proactive remediation**

Address vulnerabilities as soon as they are identified. Implement a clear process for patching and improving systems to prevent exploitation by attackers.

**5 Strengthen data protection measures**

Apply encryption, access controls, and multi-factor authentication (MFA) to protect sensitive data, particularly for mission-critical systems.

**This approach helps protect innovation and operations, minimises risk, and builds customer trust.**



# Protect Personally Identifiable Information (PII) from exposure

Ransomware attacks often target personally identifiable information (PII), causing significant consequences for both individuals and organisations.

## The exposure of PII can result in:



**Financial losses:** Individuals face heightened risks of identity theft and fraud, while organisations may be forced to compensate victims and cover the costs of addressing fraud.



**Regulatory fines:** Non-compliance with data protection regulations such as GDPR and POPIA can result in fines. For example, GDPR fines can reach up to 4% of global turnover, and POPIA fines up to R10m.



**Reputational damage:** Organisations that fail to protect PII risk losing customer trust and facing long-term reputational harm.



**Operational disruptions:** Data breaches can halt operations, especially in sectors that rely on data flow, such as healthcare and finance.

## To protect against PII exposure, organisations should take the following actions:

- **Encrypt sensitive data, both at rest and in transit:**

This prevents unauthorised access even if attackers manage to breach the network.

- **Implement multi-factor authentication (MFA):**

It was repeatedly stressed by interviewees for this report that using MFA adds an additional layer of security, making it more difficult for attackers to access systems even if credentials are compromised. It is particularly important for protecting remote access and VPN services.

- **Conduct regular security audits, vulnerability scans, and penetration tests:**

Frequent security audits help identify vulnerabilities before attackers can exploit them. Penetration testing, which simulates real-world cyberattacks, allows organisations to assess the robustness of their security measures.

- **Provide employees with ongoing training and education on recognising phishing and social engineering attacks:**

Phishing remains a common entry point for ransomware attacks. Regular employee training on recognising phishing attempts, suspicious links, and social engineering tactics is crucial for reducing human error.

- **Develop robust data backup and recovery plans to ensure data can be restored without paying a ransom:**

Organisations must have a comprehensive data backup strategy that includes regular, automated backups with associated ransomware protection, stored in separate, secure locations.

- **Adhere to regulatory requirements:**

Compliance with data protection laws such as GDPR or POPIA helps mitigate risks and reduces the likelihood of hefty fines, especially where regulatory authorities can see that every effort has been made to protect PII. Regular reviews of data handling policies ensure that organisations remain compliant.



In summary, organisations must adopt a proactive, multi-layered approach to cybersecurity to safeguard PII from ransomware attacks. By implementing robust security measures, complying with regulations, and ensuring operational resilience, companies can mitigate the risk of PII exposure and its damaging consequences.

# Conduct regular security assessments and audits

Conduct frequent risk assessments and vulnerability scans to ensure that the organisation's security posture evolves with the threat landscape. This includes penetration testing and automated monitoring tools that help identify weak points before attackers do. Regular assessments should not only focus on technical vulnerabilities but also on potential weaknesses in employee behaviour and internal processes.

## ACTIONS

1



### Schedule regular risk assessments:

Implement a quarterly or biannual schedule for comprehensive risk assessments, focusing on both external threats and internal vulnerabilities. Ensure these assessments cover technical, human, and process-related risks.

2



### Perform penetration testing:

Engage in regular penetration testing exercises to simulate cyberattacks and identify exploitable weaknesses before attackers do. These tests are often undertaken by external parties. Focus on mission-critical systems and high-risk areas.

3



### Deploy automated monitoring tools:

Use AI-driven and automated monitoring tools for continuous real-time scanning. These tools should detect anomalies and alert teams to potential vulnerabilities or threats as they emerge.

4



### Assess employee behaviour risks:

Include assessments of human behaviour, such as susceptibility to phishing attacks or failure to follow security protocols. Regularly review internal processes for gaps or outdated practices that could lead to vulnerabilities.

5



### Update and evolve security protocols:

Use insights from risk assessments to update security protocols, ensuring they evolve with new threats. Prioritise the mitigation of the most critical vulnerabilities.

6



### Integrate vulnerability scans with compliance audits:

Align vulnerability scanning with compliance requirements (e.g., GDPR, POPIA) to ensure that security measures not only address threats but also maintain regulatory adherence.

7



### Create an actionable report for stakeholders:

After each assessment, provide an actionable report detailing findings and recommendations. Include a timeline for implementing necessary improvements and assign accountability for each action item.

By following these actions, your organisation will be able to adapt its security posture proactively, stay ahead of emerging threats, and reduce the risk of costly breaches.

# Commit to proactive cybersecurity engagement

**To effectively tackle growing cybersecurity challenges, organisations must adopt a proactive approach.**

However, highlighted by every interviewee for this report, the shortage of skilled cybersecurity professionals is particularly pronounced in South Africa and across the broader Africa region, making the task even more daunting. To bridge this gap, organisations need to focus on an essential but often underutilised resource—their employees.

Comprehensive cybersecurity awareness and education are crucial in mitigating risks, particularly those stemming from accidental or negligent actions. Interviewees for this report repeatedly stressed that security awareness training should not be treated as a one-off event, but rather as an ongoing initiative, focused on changing behaviour. Regular, real-world examples of how security incidents were successfully prevented can illustrate the critical role every individual plays in protecting the organisation. This approach helps to embed cybersecurity into the organisational culture, making it a collective responsibility shared by all employees.

For smaller organisations with limited resources, affordable software and services are available to provide ongoing security education. Larger organisations, while often better equipped with tools and resources, must continue to emphasise employee engagement in cybersecurity. Interviewees pointed out that regularly showcasing the successes achieved through these efforts reinforces the importance of everyone's role in safeguarding the company's assets and data.

By making cybersecurity everyone's responsibility, businesses of all sizes can build a more resilient defence against cyber threats. Empowering employees with the knowledge and skills to recognise and prevent security breaches is not just an operational necessity—it's a strategic advantage in today's increasingly connected digital landscape.



## ACTIONS

**1 Implement continuous employee training programs**

Develop and maintain an ongoing cybersecurity awareness training and education program for all employees. Incorporate real-world examples and case studies to illustrate the impact of security breaches and the importance of vigilance.

**1****2 Embed cybersecurity into company culture**

Make cybersecurity a core element of your company's culture by regularly communicating its importance through internal channels, meetings, and leadership messaging. Ensure all employees understand their role in safeguarding the organisation's assets.

**2****3 Utilise external learning resources**

Leverage affordable cybersecurity education platforms and tools, especially for smaller organisations with limited resources. Use cloud-based solutions for scalable and continuous employee training.

**3****4 Regular security drills and simulations**

Conduct simulated phishing attacks and other cybersecurity drills to test employee readiness and identify gaps in knowledge. Use the outcomes to adjust training and improve security practices

**4****5 Regularly report and showcase successes**

Share examples of how effective cybersecurity practices have prevented potential breaches, reinforcing the importance of individual contributions. Make these reports visible to all employees to build a sense of collective responsibility.

**5****6 Create incentives for engagement**

Recognise and reward employees who consistently follow best practices and actively contribute to security efforts. Consider implementing a recognition program that highlights departments or individuals who excel in security awareness

**6****7 Develop a cybersecurity ambassador program**

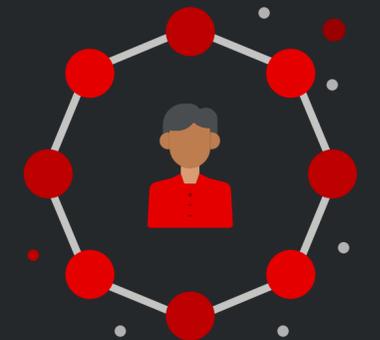
Appoint "cybersecurity ambassadors" within each department who serve as key contacts for security questions and promote awareness in day-to-day operations. These ambassadors can also help identify potential vulnerabilities from a departmental perspective.

**7****8 Leverage third-party expertise**

Where internal expertise is lacking, consider partnering with Managed Security Service Providers (MSSPs) or cybersecurity consultants to supplement your team. This approach ensures 24/7 monitoring and a higher level of expertise in incident response.

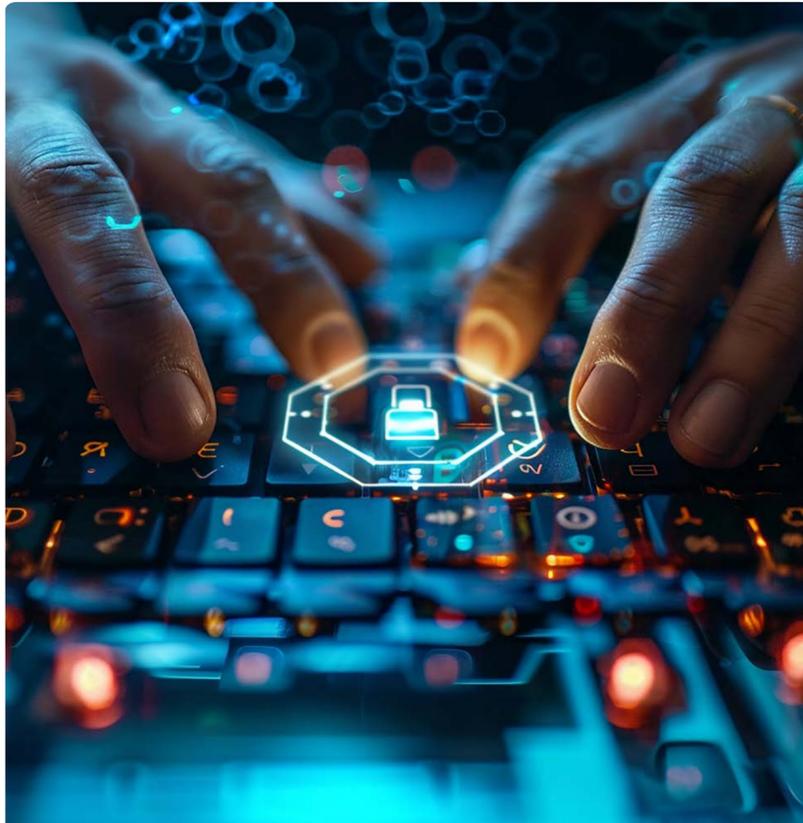
**8**

**By empowering your workforce with ongoing training, embedding cybersecurity into the culture, and leveraging external resources, your organisation can change behaviour, close the skills gap, and build a robust, proactive people-based defence against cybersecurity threats.**



# Leverage automation and advanced tools

Utilise advanced security technologies such as AI-driven threat detection, automated monitoring, and endpoint protection. These tools enable organisations to quickly detect anomalies and respond to incidents before they escalate. Automation also helps organisations stay ahead of attackers who use AI to exploit vulnerabilities more rapidly.



## ACTIONS

- 1** 
**Implement AI-driven threat detection:**  
 Deploy AI-based solutions to monitor and detect anomalies in real-time. This will allow for quicker identification and response to potential cyber threats before they escalate.
- 2** 
**Automate security monitoring:**  
 Set up automated monitoring tools that continuously check your systems for vulnerabilities, reducing the need for manual oversight and ensuring faster detection of breaches.
- 3** 
**Strengthen endpoint protection:**  
 Use automated endpoint protection systems to safeguard devices and networks, ensuring consistent monitoring and rapid response to security threats.
- 4** 
**Integrate automation into response strategies:**  
 Develop an automated incident response plan that reacts to threats in real-time, limiting damage and preventing escalation.
- 5** 
**Stay ahead of AI-driven attacks:**  
 Regularly update and enhance automation tools to counter AI-based threats used by attackers. Implement adaptive solutions that learn from previous attacks to improve future defences.

Taking advantage of automation and more, these actions ensure your organisation stays agile, proactive, and protected from increasingly sophisticated cyberattacks

# Avoid pitfalls of going it alone

**Managing every aspect of cybersecurity in-house can quickly become overwhelming, inefficient, and resource-intensive for most organisations.**

The rapidly evolving nature of cyber threats, combined with the need for constant vigilance, makes it nearly impossible for companies to handle all their cybersecurity needs internally. To address this challenge, many organisations are increasingly turning to external partners and suppliers to bolster their cybersecurity infrastructure. One interviewee commented that **“working with a partner, such as an MSSP, provides people on the ground to support the organisation and enables in-house cybersecurity staff to expand their knowledge”**.

Standard Bank spends an enormous amount on cybersecurity but still sees the virtue of not going it alone: As the Bank’s Group CIO Jörg Fischer told Tech Central: **“We spend north of R1 billion on cybersecurity. Even though we have quite a good in-house team, we also work with quite a lot of partners.**

“Service providers, particularly those specialising in managed security services, maintain robust and well-established partnerships with various technology vendors. Indeed, as previously referenced, over 90% of cybersecurity spending in Africa is sold through partners<sup>14</sup>. Partnerships are essential to the cybersecurity ecosystem. These relationships enable partners, including service providers, to offer customers a range of options and value, without the high costs or the need for in-house expertise typically required when purchasing directly.

<sup>14</sup> Canals insights, October 2024

<sup>15</sup> Omdia Cybersecurity Decision Maker Survey 2024 n=964

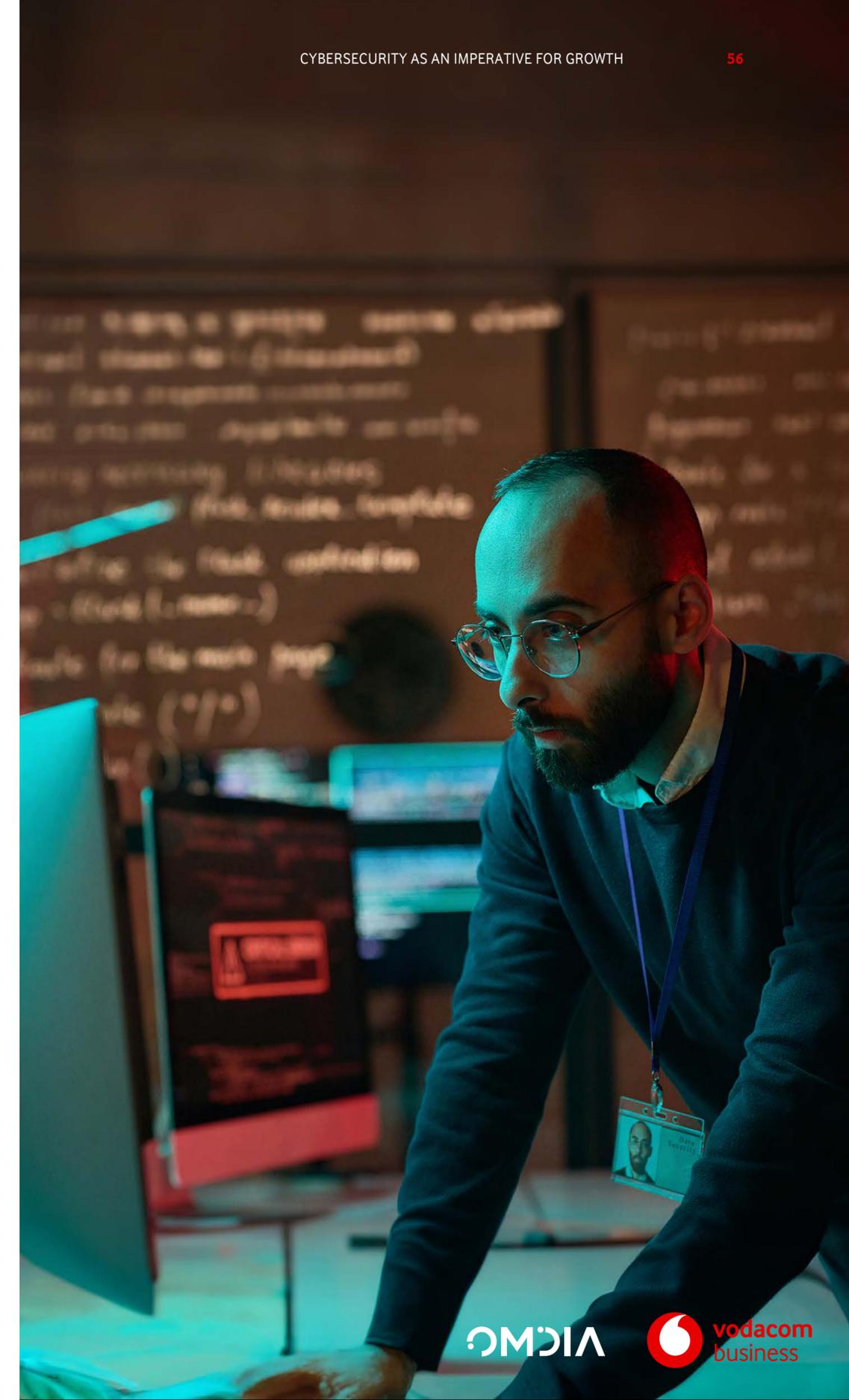
Omdia research notes that 55% of organisations outsource components of their cybersecurity operations, while 56% engage external providers for incident escalation<sup>15</sup>. Utilising external providers is now commonplace.

In Africa, this trend is even more pronounced. Managed security services are projected to be the leading investment area in cybersecurity, with 61% of organisations planning to further invest in this domain in 2025<sup>16</sup>. A further 22% will maintain their existing investment in managed security services over the same period. This surge highlights the growing recognition of the value that specialised external support brings to an organisation's security infrastructure. External partners offer customised capabilities, tailored to meet the specific needs of each customer organisation, ensuring a more robust and responsive security posture.

By collaborating with specialised external providers with the skillsets that are often in short supply elsewhere<sup>17</sup>, organisations can access advanced expertise and cutting-edge technologies that are often unavailable inhouse. This partnership allows companies to enhance their cybersecurity capabilities, mitigate risks more effectively, and focus on their core business functions. Moreover, outsourcing can offer cost advantages, as building and maintaining an internal cybersecurity team is often more expensive and unpredictable. Engaging external providers can result in faster detection of cyber threats, with many specialist vendors ensuring compliance with relevant regulations on behalf of their clients.

<sup>16</sup> Omdia IT Enterprise Insights 2024-25 n=131

<sup>17</sup> Omdia Cybersecurity Decision Maker Survey 2024 n=964 46% of respondents highlighted “workforce shortage” in their top three issues



Beyond cost savings, external partners provide access to a variety of support resources, such as paid cybersecurity assessments and clinics, which help organisations ramp up their cybersecurity practices more quickly and efficiently. Interviewees commented that the insight and expertise of partners is incredibly helpful to customer organisations developing their cybersecurity capabilities. One organisation, for example, benefited from an external provider's support in the following areas:



**Access to expertise not available in-house**



**Round-the-clock monitoring of security events and incidents**



**Up-to-date information on security threats, vulnerabilities, and attack methodologies**



**Enhanced threat detection through the use of AI and automation**

Navigating today's cybersecurity landscape alone can leave organisations vulnerable to threats and attacks. Engaging external expertise is not only beneficial—it's essential. By leveraging external support, companies can strengthen their defences, remain compliant with regulations, and ensure long-term resilience in the face of evolving cyber risks.

## ACTIONS

**Partner with a MSSP:**

Leverage MSSPs to handle round-the-clock monitoring, threat intelligence, and incident response. This provides access to industry-leading expertise and tools, enabling faster detection and mitigation of cyber threats.

**1****Identify core cybersecurity needs:**

Assess your internal capabilities to determine which cybersecurity functions can be effectively handled in-house and which should be outsourced. Focus on areas where external expertise is critical, such as advanced threat detection or incident escalation.

**2****Integrate AI and automation tools:**

Partner with external providers that offer AI-driven cybersecurity tools, enhancing real-time detection and response capabilities. This reduces manual oversight and increases the accuracy of threat identification.

**3****Customise security solutions:**

Work with specialised external vendors to create tailored cybersecurity solutions that align with your organisation's specific needs and risk profile. Ensure these solutions evolve with the threat landscape.

**4****Ensure regulatory compliance:**

Collaborate with external providers to ensure compliance with relevant data protection and cybersecurity regulations, such as GDPR and POPIA. Many MSSPs include compliance management as part of their service offerings.

**5****Conduct regular security assessments:**

Schedule regular paid cybersecurity assessments and clinics through external partners to evaluate your security posture and address vulnerabilities promptly.

**6****Optimise costs through outsourcing:**

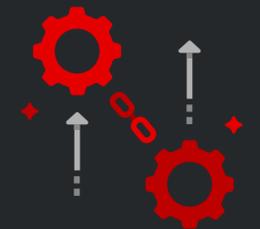
Use outsourcing to avoid the high costs of building and maintaining an internal cybersecurity team. This allows for predictable, scalable investment in security without sacrificing quality or speed of response.

**7****Maintain continuous communication:**

Establish strong communication protocols with your external providers to ensure your security operations remain integrated with your internal processes. Regular reporting and meetings will help maintain alignment with your evolving security needs.

**8**

**Cybersecurity measures must also extend beyond the organisation's internal operations to include the supply chain. As businesses grow, ensuring that external partners meet the same rigorous cybersecurity standards is essential. By partnering with external providers, organisations can reduce costs, improve threat detection, and remain compliant with evolving regulations.**

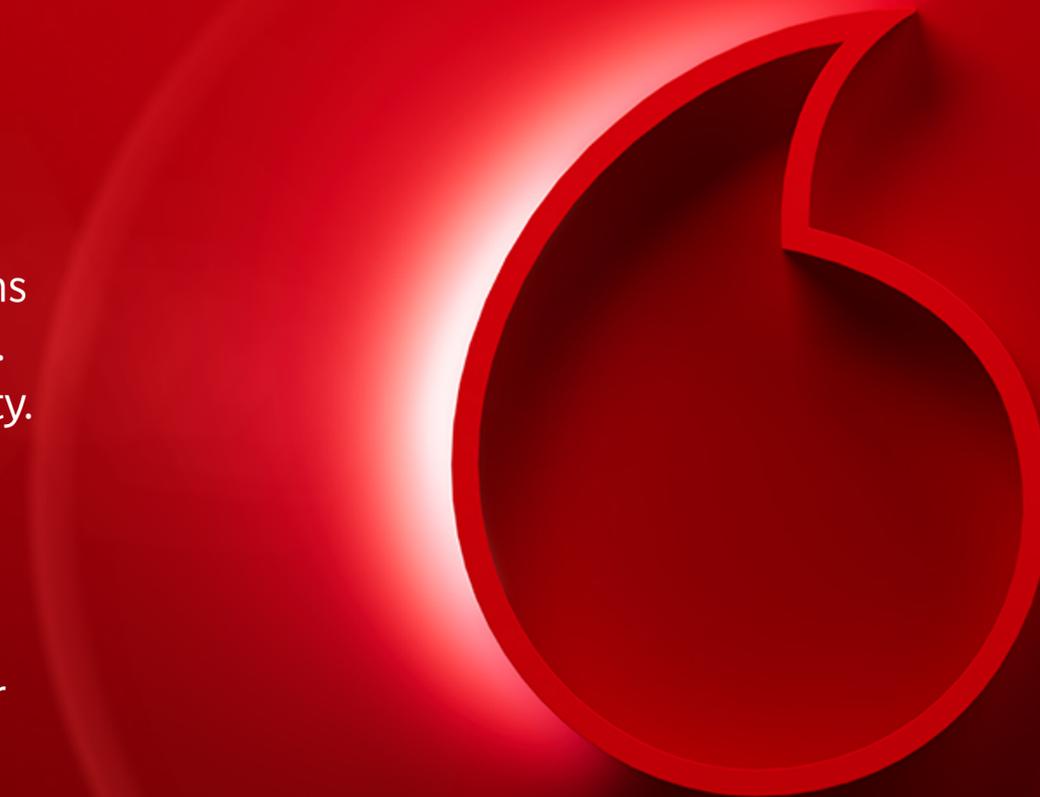


# Conclusion

## **Cybersecurity is more than just a technological issue; it's a cornerstone of trust.**

By embedding robust cybersecurity strategies into their operations, organisations can safeguard their reputation while unlocking new digital growth opportunities. This is not only a critical responsibility but also a substantial business opportunity. Although human error remains a persistent challenge, fostering a culture of vigilance can be a decisive factor.

With the right safeguards in place, businesses can confidently drive innovation and launch new digital products and services, secure in the knowledge that their cybersecurity infrastructure underpins both resilience and progress. But is your organisation truly leveraging cybersecurity as a strategic growth enabler? The time to reevaluate and act is now.



## About us



### About Vodacom Business

Vodacom is a leading and purpose-led African connectivity, digital and financial services company, and we are celebrating our

## 30th anniversary

Vodacom Business is the enterprise division of Vodacom Group Limited.

Vodacom Business South Africa was launched in 2009 to provide the skills and capabilities that can help companies turn themselves into digital businesses.

We are a challenger company with something to prove: very focused on working alongside our customers to get results. We offer a comprehensive suite of services designed to help business of all sizes enhance their operations through advanced technology solutions.

<https://www.vodacombusiness.co.za/>

<https://help.vodacom.co.za/business/contactus>



### About Omdia consulting

Omdia is a market-leading data, research and consulting business focused on helping digital service providers, technology companies and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development and go-to-market initiatives.

Our unique combination of authoritative data, market analysis and vertical industry expertise is designed to empower decisionmaking, helping our clients profit from new technologies and capitalise on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

### Analyst



**Maxine Holt**  
Vice President, Enterprise Research

Maxine has spent her entire career as an IT and security professional and has been at Omdia since 2018. Maxine is the lead architect of the Omdia Cybersecurity Ecosystem. Maxine built her in-depth cybersecurity expertise initially at the Information Security Forum (ISF), developing thought-leading security research for ISF Members. Prior to the ISF, Maxine spent 15 years in technology research at Ovum, having started her career as a software developer in the financial services industry and working in consulting for the financial services and internet sectors. Maxine was named the IAR Industry Analyst of the Year, EMEA, 2023 and is a regular speaker at events, also contributing thought-leading content to high-profile publications in cybersecurity and technology.

#### COPYRIGHT NOTICE AND DISCLAIMER

Omdia is a registered trademark of Informa PLC and/or its affiliates. All other company and product names may be trademarks of their respective owners. Informa PLC registered in England & Wales with number 8860726, registered office and head office 5 Howick Place, London, SW1P 1WG, UK. Copyright © 2024 Omdia. All rights reserved. The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact. The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result. Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials. To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.



Further together