CYBERSECURITY RESILIENCE OF SOUTH AFRICA'S PUBLIC SECTOR

REPORT 1: CYBERSECURITY AWARENESS AND PREPAREDNESS

Compiled by: Zubeida Dawood, Avuya Shibambu, Thuli Mkhwanazi, Oyena Mahlasela, Errol Baloyi and Noku Siphambili

In today's digital age, cybersecurity is a paramount concern for all South African organisations, particularly public sector institutions that hold sensitive citizen data and government information. This report delves into survey responses from public sector entities within South Africa to gain a clearer picture of their current state of cybersecurity awareness and preparedness. The survey received responses (N = 291) from a diverse range of South African public sector institutions, including government departments, municipalities and other public entities. This broad representation provides valuable insights into the cybersecurity posture of the South African public sector.

This report can be used to identify areas for improvement, prioritise resource allocation and ultimately strengthen the overall cybersecurity resilience of public institutions in South Africa.

This initial report (Report 1 on 15 April 2024) lays the groundwork by examining the current state of cybersecurity awareness and preparedness within participating institutions. In the following weeks, two additional reports will be released on 22 and 29 April 2024, respectively. Shifting focus, Report 2 dives into the specific cybersecurity policies and practices implemented by public sector institutions. The final report examines how public sector institutions maintain compliance with cybersecurity regulations and strive for ongoing improvement.

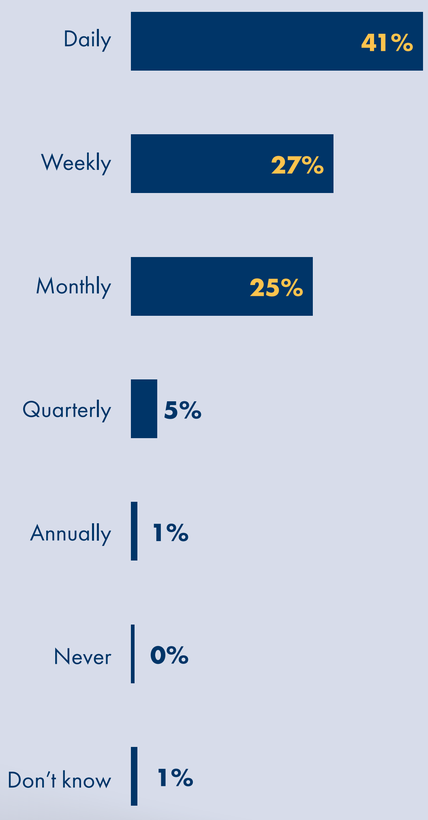
KEY TAKEAWAYS:

- Public sector institutions in South Africa conduct cybersecurity risk assessments fairly frequently, with 68% doing so at least monthly;
- A significant number (47%) have experienced one to five cybersecurity incidents in the past year, highlighting the prevalence of cyber threats;
- Malware and phishing attacks are the most common cyber threats faced by these institutions;
- Despite feeling well-prepared (64% very prepared), there is still a small percentage (6%) of public sector institutions that lack confidence in handling cybersecurity incidents;
- The positive news is that 89% of institutions have a formal cybersecurity incident response plan;
- Encouragingly, a combined 64% review their response plans at least quarterly, indicating a proactive approach; and
- While there is a positive trend in employee cybersecurity awareness training, there is still room for improvement, with 7% not training any employees and 32% training only 1-25%.

DATA ANALYSIS AND INSIGHTS

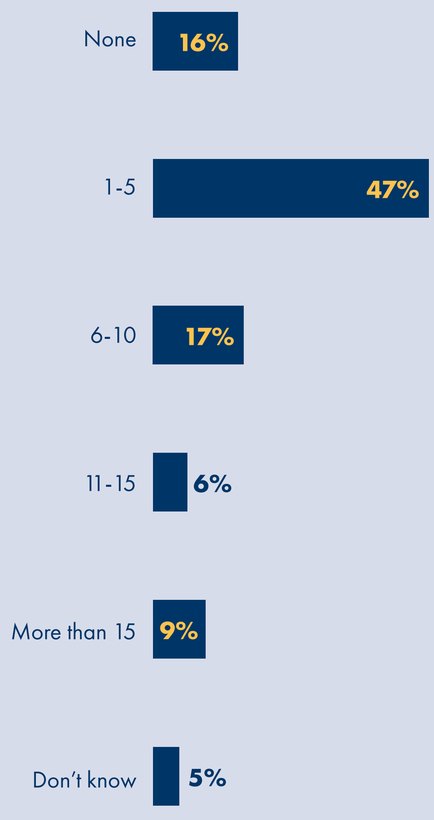
Risk assessment frequency: The frequency of risk assessments undertaken by public sector organisations is as follows:

How frequently are cybersecurity risks assessed and monitored in your organisation?



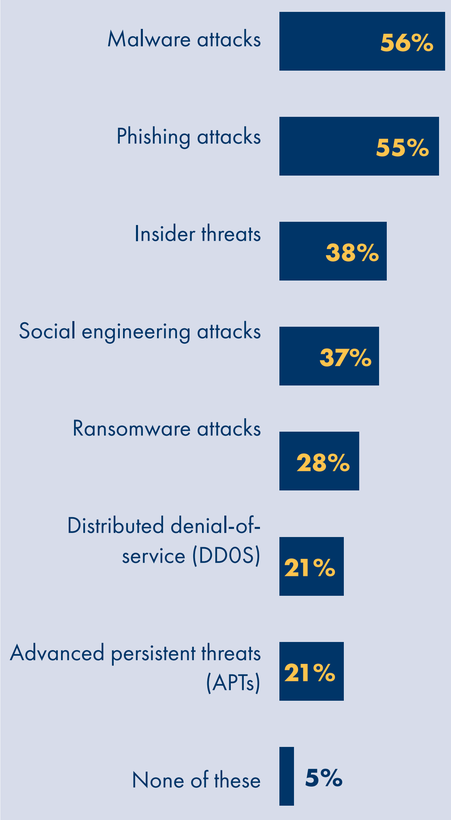
Cybersecurity incidents: The frequency of incidents that occurred is as follows:

How many cybersecurity incidents have occurred in the past year in your organisation?



Cybersecurity threat landscape: Malware and phishing attacks are the most common threats faced by South African public sector institutions.

What types of cybersecurity threats does your organisation face? Please select all that apply.



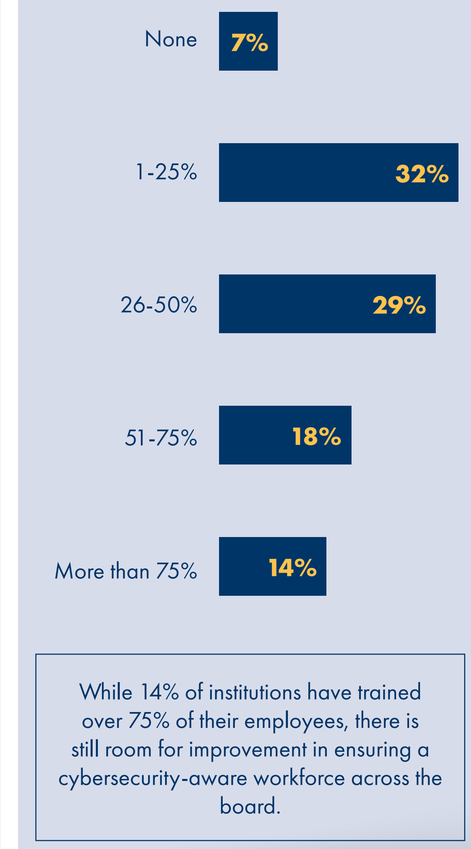
Preparedness and response: A significant majority (64%) of public sector institutions feel very prepared to handle cybersecurity incidents.

How prepared is your organisation to handle cybersecurity incidents?

To reinforce this thinking, it was found that 89% of public sector institutions have a formal cybersecurity incident response plan in place. It is encouraging to note that a combined 64% of institutions review their incident response plans at least quarterly.

Employee training: Cybersecurity awareness training occurs as follows:

How many employees in your organisation have received cybersecurity awareness training in the past year?



While 14% of institutions have trained over 75% of their employees, there is still room for improvement in ensuring a cybersecurity-aware workforce across the board.

For more information, visit **www.csir.co.za**

science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

CSIR
Touching lives through innovation

CYBERSECURITY RESILIENCE OF SOUTH AFRICA'S PUBLIC SECTOR

REPORT 2: HIGHLIGHTING CYBERSECURITY POLICIES AND PRACTICES IMPLEMENTED BY ORGANISATIONS

Compiled by: Zubeida Dawood, Avuya Shibambu, Thuli Mkhwanazi, Oyena Mahlasela, Errol Baloyi and Noku Siphambili

The initial report (Report 1) laid the groundwork by examining the current state of cybersecurity awareness and preparedness within participating institutions. Shifting focus, Report 2 dives into the specific cybersecurity policies and practices implemented by public sector institutions. The following final report will examine how public sector institutions maintain compliance with cybersecurity regulations and strive for ongoing improvement.

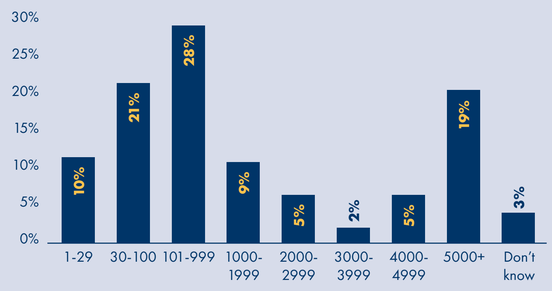
KEY TAKEAWAYS:

- It is comforting to note that 95% of the surveyed organisations have an Information Security policy for Access Management in place;
- 50% of organisations perform automatic patches and updates, while only 1% do so only after an incident has occurred;
- 95% of the organisations have a data backup and recovery plan in place;
- 56% of the organisations have experienced some data breaches over the past year;
- In conjunction with other methods, the regular assessment of third-party vendors for cybersecurity risks is the most used method by 74% of organisations;
- While 86% of the organisations conduct regular vulnerability testing, 14% do not, which poses a risk as attackers have more chances of compromising their systems;
- 17% of the organisations run annual security assessments on their networks and systems, while 25% of them run them monthly. It is alarming that 1% shared that they do not run any security assessments;
- It is noteworthy that all the surveyed organisations use more than one method to protect against malware and ransomware attacks, with anti-malware and anti-virus software being the most used method (78% of organisations use it);
- User awareness training is one of the methods that most organisations (71%) use to detect and respond to phishing attacks;
- Encryption is one of the ways organisations protect sensitive data and information, and it is used by 76% of organisations, followed closely by access controls at 75%; and
- 80% of organisations use access control to detect and respond to insider threats, in conjunction with user monitoring and data loss protection.

DATA ANALYSIS AND INSIGHTS

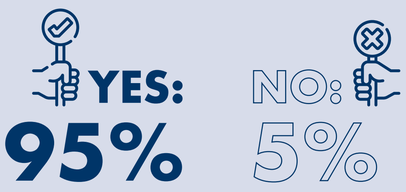
Organisation size: The number of employees currently employed at the organisation:

Approximately, how many employees are currently employed by your organisation (both part-time and full-time employees)?



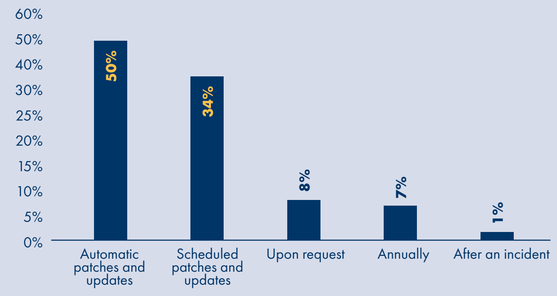
Information Security Policy for Access Management: 95% of organisations do have one.

Does your organisation have an information security policy in place for managing access to information systems?



Security patch and update application frequency: 50% of organisations perform automatic patches and updates.

How often are security patches and updates applied to your organisation's systems?

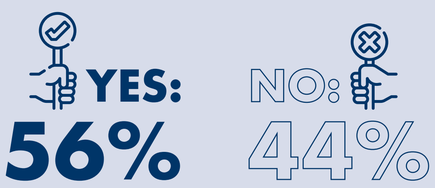


Data backup and recovery plan: 95% of the organisations do have a data backup and recovery plan in place.

Does your organisation have a data backup and recovery plan in place?

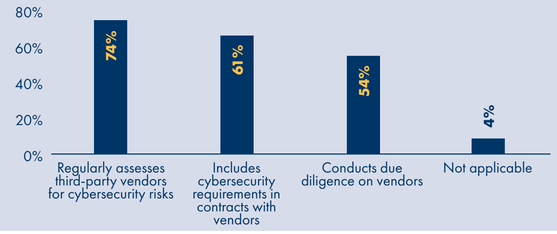
Data breaches experienced (past year): 56% of organisations have experienced some data breaches over the past year.

Has your organisation experienced any data breaches in the past year?



Methods for identifying and managing third-party cybersecurity risks: Among other methods, most organisations (**74%**) regularly assess third-party vendors for cybersecurity risks.

How does your organisation identify and manage third-party cybersecurity risks? Please select all that apply.



Regular vulnerability testing: While **86%** of organisations conduct regular vulnerability tests, **14%** do not.

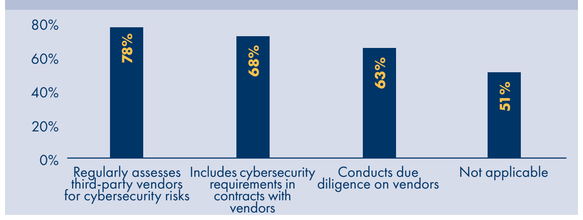
Does your organisation conduct vulnerability testing on a regular basis?

Security assessment frequency (networks and systems): 25% of organisations run monthly security assessments on their networks and systems.

How often are security assessments conducted on your organisation's networks and systems?

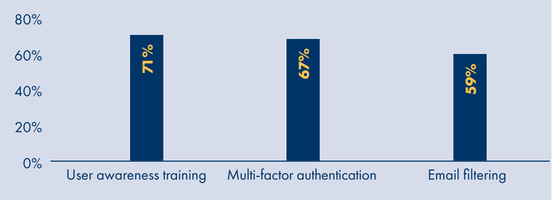
Measures to protect against malware/ ransomware attacks: Most (**78%**) organisations make use of anti-malware and anti-virus software to protect against malware and ransomware attacks, amongst other measures.

What measures does your organisation have in place to protect against malware and ransomware attacks? Please select all that apply.



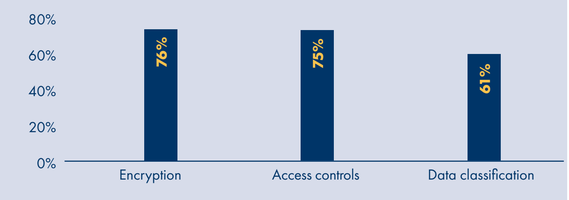
Methods to detect and respond to phishing attacks: User awareness training is one of the methods that most organisations (**71%**) use to detect and respond to phishing attacks.

How does your organisation detect and respond to phishing attacks? Please select all that apply.



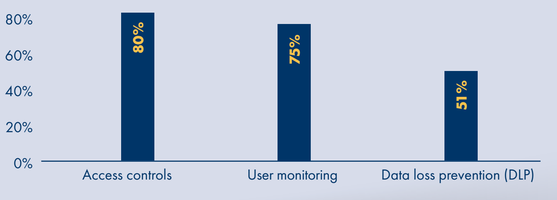
Methods to protect sensitive data and information: Encryption is used by **76%** of organisations to protect sensitive data and information.

How does your organisation protect sensitive data and information? Please select all that apply.



Measures to detect and respond to insider threats: Of the three measures provided below, **80%** of organisations use access control to detect and respond to insider threats.

What measures does your organisation have in place to detect and respond to insider threats? Please select all that apply.



science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

For more information, visit **www.csir.co.za**

CSIR
Touching lives through innovation

CYBERSECURITY RESILIENCE OF SOUTH AFRICA'S PUBLIC SECTOR

REPORT 3: EXAMINING HOW ORGANISATIONS MAINTAIN COMPLIANCE AND STRIVE FOR IMPROVEMENT

Compiled by: Zubeida Dawood, Avuya Shibambu, Thuli Mkhwanazi, Oyena Mahlasela, Errol Baloyi and Noku Siphambili

KEY TAKEAWAYS:

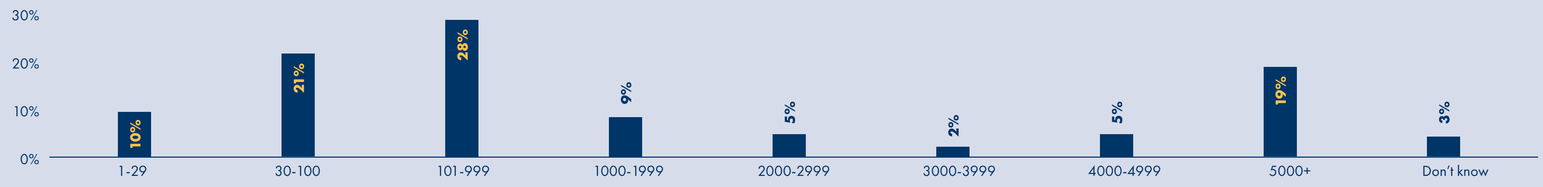
- Organisations employ various methods to ensure they comply with regulations and standards, and 68% of them use regular assessments of their compliance levels against what is required;
- With the prevalence of cybersecurity attacks, it is good to note that 79% of organisations perform regular reviews and updates of their cybersecurity policies and procedures;
- Most organisations consider the importance of implementing various frameworks and standards, with the NIST Cybersecurity Framework being popular among 71% of them. Unfortunately, 5% reported that they do not follow any cybersecurity frameworks or standards in their organisations;
- All organisations review their policies and procedures over various intervals ranging from monthly, quarterly, bi-annually and annually. A majority of them (30%) perform the reviews quarterly;
- 43% of organisations use automated software tools for mapping their cybersecurity controls to available frameworks and standards;
- As a method to measure their cybersecurity posture against frameworks and standards, 41 % of organisations conduct regular self-assessments;
- Given the importance of cybersecurity in running an organisation, it is crucial that organisations allocate some funds to this area. They use various methods to invest in their cybersecurity, with 70% of them allocating resources based on the risks and maturity levels identified in the frameworks or standards;
- As businesses have various stakeholders, it is important that they demonstrate their compliance with cybersecurity regulations. 65% of organisations use third-party reports or certificates for this purpose;
- Once an incident has occurred and has been assessed, it is good practice to incorporate the lessons learnt into the organisation's compliance. 66% of organisations regularly update their cybersecurity policies and procedures to incorporate the lessons learnt, while 44% use them as part of ongoing cybersecurity awareness and training for their employees.

The previous reports in the series focused on awareness and compliance, respectively. This report delves into the methods that organisations employ to remain compliant and strive to improve their posture.

DATA ANALYSIS AND INSIGHTS

Organisation size: The number of employees currently employed at the organisation:

Approximately, how many employees are currently employed by your organisation (both part-time and full-time employees)?



Methods for ensuring compliance with regulations and standards: 68% of organisations perform regular compliance assessments with regulations and standards.

How does your organisation ensure compliance with cybersecurity regulations and standards?

Regularly assesses compliance with regulations and standards: **68%**

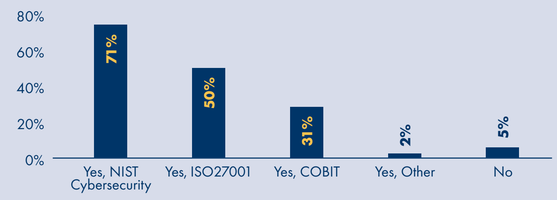
Appoints a compliance officer to oversee compliance efforts: **32%**

Steps taken to improve cybersecurity posture: Most organisations (**79%**) perform regular reviews and update their cybersecurity policies and procedures as part of the steps to improve their cybersecurity posture.

What steps is your organisation taking to continuously improve its cybersecurity posture? Please select all that apply.

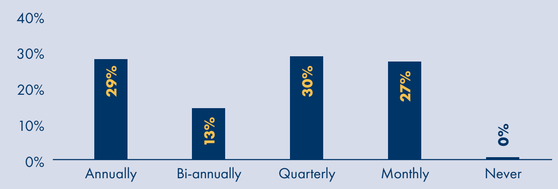
Cybersecurity Frameworks or Standards Followed: 71% of organisations follow NIST, among other cybersecurity frameworks or standards.

Does your organisation follow a cybersecurity framework or standard? Please select all that apply.



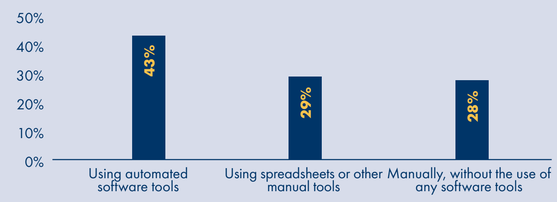
Cybersecurity policy and procedure review frequency: 30% of organisations review their cybersecurity policies and procedures quarterly.

How often does your organisation review and update its cybersecurity policies and procedures to align with cybersecurity frameworks or standards?



Methods for mapping cybersecurity controls to frameworks or standards: 43% of organisations use automated software tools for mapping their cybersecurity controls to frameworks and standards.

How does your organisation map its cybersecurity controls to the requirements of cybersecurity frameworks or standards?



Methods for measuring cybersecurity posture against frameworks or standards: 41% of organisations regularly conduct self-assessments against frameworks or standards to measure their posture.

How does your organisation measure its cybersecurity posture against cybersecurity frameworks or standards?

Cybersecurity investment prioritisation method: 70% of organisations allocate resources based on the risks and maturity levels they have identified in the frameworks/standards as their cybersecurity investment prioritisation method.

How does your organisation prioritise its cybersecurity investments based on the requirements of cybersecurity frameworks or standards?

Allocates resources based on the risk and maturity levels identified in the framework or standard: **70%**

Allocates resources based on a qualitative assessment of the organisation's cybersecurity posture: **30%**

Methods for demonstrating compliance to external stakeholders: 65% of organisations provide reports or certificates from a third-party auditor to demonstrate compliance with their external stakeholders.

How does your organisation demonstrate its compliance with cybersecurity frameworks or standards to external stakeholders?

Provides reports or certifications from a third-party auditor: **65%**

Provides self-assessment reports or certifications: **35%**

Incorporation of lessons learnt from incidents into compliance: 66% of organisations perform regular updates of their cybersecurity policies and procedures to address the lessons learnt from incident reviews.

How does your organisation incorporate lessons learned from cybersecurity incidents into its compliance efforts with cybersecurity frameworks or standards?

Regularly updates its cybersecurity policies and procedures to address the findings of incident reviews: **66%**

Incorporates the findings of incident reviews into ongoing cybersecurity awareness training for employees: **34%**

For more information, visit **www.csir.co.za**

science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

CSIR
Touching lives through innovation