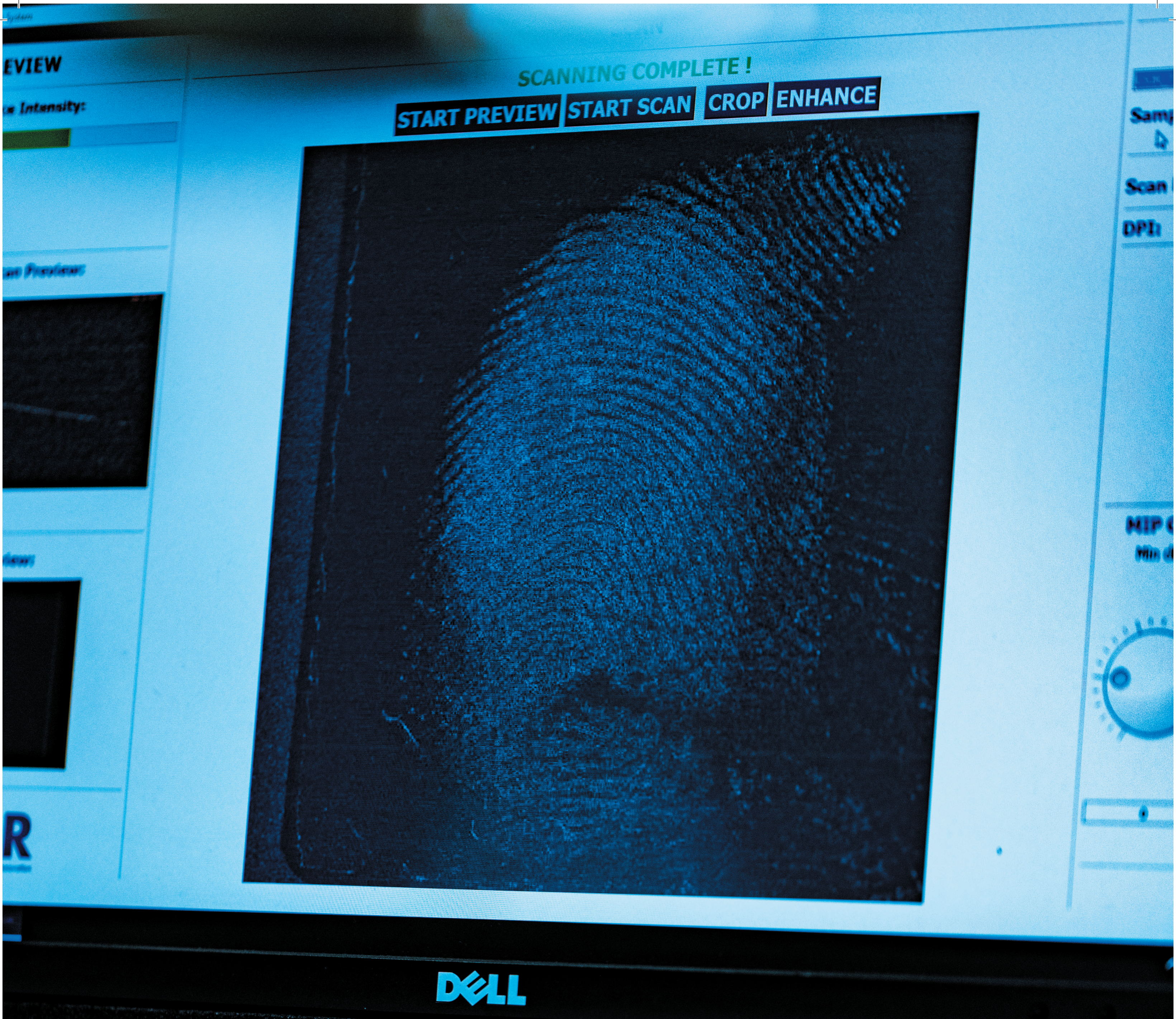


CSIR INFORMATION AND **CYBERSECURITY CENTRE**

The CSIR Information and Cybersecurity Research Centre developed, piloted and commercialised the innovative VeristicPrint Biometric System. This marks the first such achievement for the centre since its inception. The system is a contactless fingerprint recognition software solution that enables any digital device, such as a smartphone or webcam, to function as a fingerprint scanner.

The system is made up of three modules:

1. *Contactless Acquisition Module;*
2. *Feature Extraction Module; and*
3. *Hash Matching Module.*

CSIR
Touching lives through innovation

ABOUT THE CSIR INFORMATION AND CYBER SECURITY RESEARCH CENTRE

Established in 2019, the CSIR Information and Cyber Security Research Centre is a consolidation of all CSIR research and development (R&D) capabilities in cybersecurity, information security and identity authentication. These capabilities were developed over decades of working for the Department of Defence and, over the last ten years, for government departments and agencies, such as the Department of Communications and Digital Technologies, state-owned enterprises and private sector players.

The centre aims to support industry, contribute to an efficient, secure and capable state and grow cybersecurity capacity and capabilities in the country. It also develops systems and solutions that are relevant to the local context and makes them available for commercialisation, which is in line with CSIR's strategic focus on industrialisation.

The CSIR has a recognised track record locally and abroad, based on its work with and support for numerous stakeholders and institutions. Since the nineties, as cyberspace became everyone's playground, several technologies were brought to local users. These include antivirus software and an early warning detection system for small businesses encompassing both software and hardware components. A major achievement was a CSIR-developed encryption solution (encoder/decoder) that led to the creation of the pay-TV giant M-Net.

Innovation is homegrown. Initiated by the CSIR and collaborators in the public and private sectors, test and evaluation platforms and cybersecurity educational and training packages have been prototyped, and some have been implemented in operational environments.

With significant experience in R&D, product innovation and capability development, the CSIR is well positioned to lead the building of a robust, agile and formidable national cybersecurity capability and capacity, as well as to foster innovation for a thriving future industry.

The centre's focus areas are:

- Securing ICT systems;
- Combating cybercrime;
- Cyberwarfare;
- Identity management;
- Awareness and human capital development
- Governance, risk and compliance, and
- Embedded security.

www.csir.co.za

FOREWORD

Local is best: Why home-grown technologies and capabilities are needed to advance South Africa's cybersecurity technology sovereignty

In an era where digital transformation is exponentially accelerating, cybersecurity has become a dominant concern worldwide. As the digital landscape evolves, so do the threats that target critical infrastructure, sensitive data, personal information and national security. Against this backdrop it is of paramount importance for nations to focus on the development of home-grown cybersecurity technologies and capabilities to gain – and retain - strategic advantage. The CSIR's Information and Cybersecurity Centre, through the support and partnerships with state entities such as the South African Department of Science and innovation (DSI), is investing in the development and nurturing the nations' local cybersecurity capabilities. Centre Manager, Dr Jabu Mtsweni and his team have crystalised the levers and target interventions to drive this mission.

SOVEREIGNTY AND NATIONAL SECURITY

Relying on foreign technologies can expose a country to significant vulnerabilities as these can have backdoors or hidden vulnerabilities that adversaries can exploit. By developing home-grown technologies, countries can maintain absolute control over their critical systems and data. Thus, ensuring that security measures align with national interests and are free from external interests.

CUSTOMISATION AND ADAPTABILITY

Every nation has unique cybersecurity needs based on its specific threat landscape, regulatory environment and infrastructure. Home-grown technologies allow for greater customisation and adaptability to meet these specific local requirements.

ECONOMIC BENEFITS AND JOB CREATION

Investing in the development of home-grown cybersecurity technologies and capabilities has significant benefits in terms of fostering the growth of local technology industry, creating jobs, and stimulating innovation.

A critical element is building a skilled national workforce capable of developing advance cybersecurity solutions – now and in the future.

Not only supplying to local need, development of technologies for the export market opens new economic opportunities and global acclaim and competitiveness.

PROMOTING INNOVATION AND RESEARCH

Localising technology development drives innovation and research. Thus, encouraging academic institutions, research councils, public and private industries to invest in the development of advanced cybersecurity technologies and capabilities, pushing through to new levels of ingenuity.

WHAT ROLE DOES THE CENTRE PLAY IN THESE OBJECTIVES?

The CSIR's Information and Cyber Security Centre, through the support provided by the Department of Science and Innovation, has embarked on R&D themes that resonate with these goals and focus capability development in areas such as authentication, detection and analysis, and governance and legal compliance. These focal points include:

1. **Enabling integrated and secure identity authentication:** the development of integrated identity as a service capability for the public sector.
2. **ZeroTrust authentication:** building foundational capability to enable continuous and efficient authentication, validation, and authorisation of users and devices across trusted and untrusted networks.
3. **Threat landscape and situational awareness:** development of low-cost capabilities to enable contextual threat landscape and situational awareness using data security analytics supported by Artificial Intelligence/Machine Learning and other emerging technologies.
4. **Low-cost early warning threat detection:** development of low-cost algorithms, hardware, and software for early warning cyber threat detection.
5. **Formalising threat intelligence sharing** development of web-based threat intelligence sharing tools to enable the sharing of indicators of compromise.
6. **Toolkits for enhancing compliance to regulatory requirements:** enhancing the protection of personal information composed of diverse instruments and templates, and tools for promoting information and cybersecurity compliance to legal and regulatory requirements across different jurisdictions.

Successes in developing home-grown cybersecurity technologies is driven by collaboration and innovation. The CSIR works closely with academic institutions, industry partners, and government agencies to leverage diverse expertise and resources. This collaborative approach leads to a better understanding of emerging threats, and continuously evolution and improvement of responding solutions. Not least of which is the investment made in training and developing cybersecurity professionals, ensuring a sustainable pipeline of talent for the republic for the future.

All this in the interest of a safe cyber-SA.

By Dr Jabu Mtsweni
Dr Jabu Mtsweni, Head of the CSIR Information and Cyber Security Centre, CSIR Chief Researcher, NRF-Rated Researcher (C2), Certified Cybersecurity Manager, Research Fellow at the Stellenbosch University, Technical Leader of the National Policy Data Observatory; Member of the International Telecommunication Standards body (Study Group 7: cyber security. Recently honoured as one of top 50 Cybersecurity Professionals in South Africa, amongst his accomplishments.

CYBERSECURITY SKILLS

With its walls adorned with colourful code diagrams and ethical hacking mottos, the CSIR Cybersecurity Learning Factory is certainly not a typical corporate environment. Here, the battle against cybercrime is not waged in sterile server rooms but in a simulated digital world teeming with virtual machines and controlled chaos.

Meet Mamello, a recent computer science graduate with a thirst for adventure. Cybersecurity had always intrigued her – the constant game of cat and mouse between defenders and attackers. Arriving at the learning factory as a trainee came with a mix of excitement and apprehension.

It was a bustling environment – trainees in headsets hunched over workstations, their faces illuminated by the glow of multiple screens. Instructors, veterans of the South African cyber-defence scene, barked instructions and monitored progress. A prevalent atmosphere of urgency, a controlled panic that mimicked the real-world pressure of a cyberattack.

Mamello's first course was in network defence, which covered network vulnerabilities and intrusion detection systems. She was trained to adopt a hacker's mindset, identifying weaknesses in firewalls and exploiting them in a safe, controlled environment. Over time, Mamello excelled in the learning factory's intense atmosphere, learning about social engineering, phishing attacks and malware analysis, with a specific focus on the threats relevant to the South African landscape. She participated in simulated cyberwarfare exercises, defending critical infrastructure from coordinated attacks launched by her classmates. Trainees are constantly challenged and introduced to cutting-edge techniques and emerging threats.

Then, the factory received an unexpected challenge when a major South African government department – a regular partner in their training exercises – was hit by a real-time cyberattack. The factory's systems were configured to mirror the department's network, and the trainees were tasked with responding to the attack in real time, under the watchful eyes of the Security Operations (SOC) team. Two well-experienced SOC analysts monitored the trainees' every move, ready to offer guidance and assess their response.

Mamello, now a seasoned trainee, found herself at the forefront of the defence. Adrenaline pumping, she analysed system logs, identified suspicious activity and patched vulnerabilities. The pressure mounted as the clock ticked with every failed login attempt and every suspicious file transfer. Finally, after hours of intense work, Mamello and her team managed to contain the simulated attack.

The department's SOC team was impressed by the trainees' performance and Mamello's initial nervousness was replaced by a newfound confidence. The factory had not only equipped her with knowledge but had also given her the practical experience and the battle-tested spirit she needed to succeed in the ever-evolving world of cybersecurity. As Mamello walked out of ICSC that day, she knew this was just the beginning of her journey as a cyber defender, forever grateful for the unique learning ground that had prepared her for the real fight.

For more information contact:
Mamello Mtshali, *MMtshali3@csir.co.za*
Mpho Letshwenyo, *mletshwenyo@csir.co.za*

RESEARCH REPORT:
CYBERSECURITY RESILIENCE OF SOUTH AFRICA'S PUBLIC SECTOR

REPORT 1: *CYBERSECURITY AWARENESS AND PREPAREDNESS*

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. It also identifies areas for improvement, priorities for resource allocation, and ultimately ways to strengthen the overall cybersecurity resilience of public institutions in South Africa.

This first report, lays 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 third report examines how public sector institutions maintain compliance with cybersecurity regulations and strive for ongoing improvement.

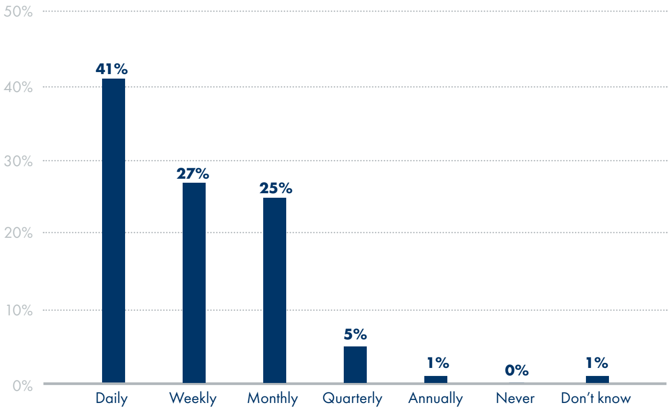
Key Takeaways

- 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 1-5 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's 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.
- While there's a positive trend in employee cybersecurity awareness training, there's still room for improvement, with 7% not training any employees and 32% training only 1-25%.

DATA ANALYSIS AND INSIGHTS

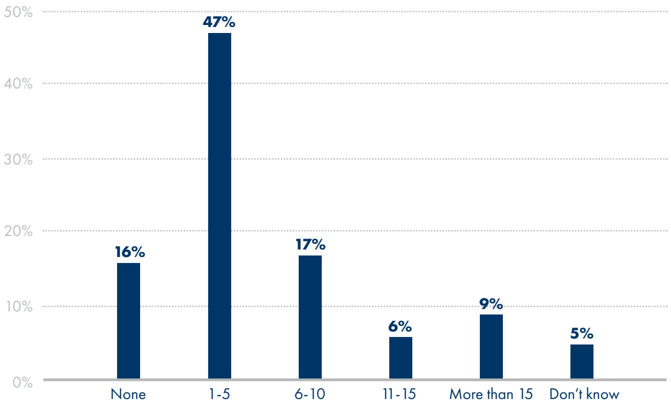
Risk Assessment Frequency: The frequency of risk assessments undertaken by public sector organisations is as follows.

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



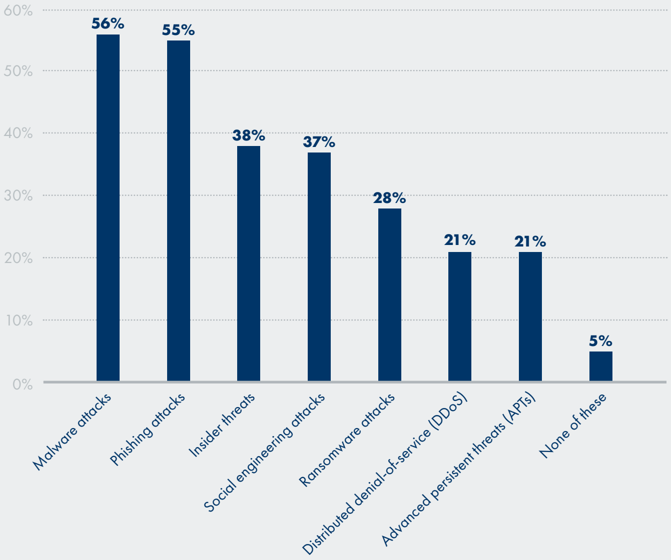
Cybersecurity Incidents: The frequency of incidents occurred is as follows.

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



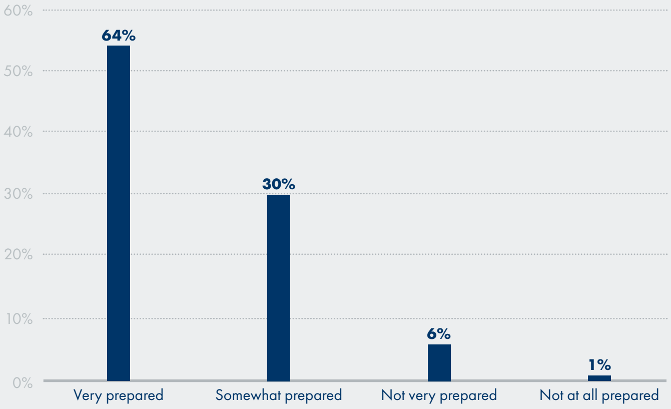
Cybersecurity threat landscape: Malware and phishing attacks are the most common threats faced by South African public sector institutions.

» *What type 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.

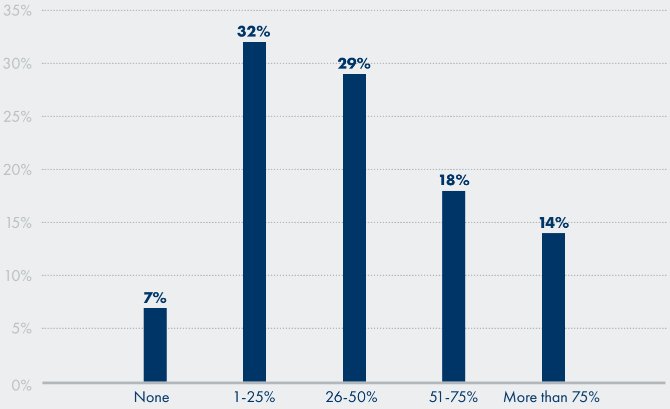
» *How prepared is your organisation to handle cybersecurity incidents?*



To reinforce this thinking, it was found that 89% of public sector institutions have a formal cybersecurity incident response plan in place. It's 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's still room for improvement in ensuring a cybersecurity-aware workforce across the board.

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

REPORT 2: *HIGHLIGHTING THE CYBERSECURITY POLICIES AND PRACTICES IMPLEMENTED BY ORGANISATIONS*

Following from a survey into the current state of cybersecurity awareness and preparedness within the public sector, focus now shifts to the specific cybersecurity policies and practices implemented by such institutions.

Key Takeaways:

- It is comforting to note that 95% of the survey participants stated that they do have an information security policy for access management.
- 50% of the organisations perform automatic patches and updates while 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 the organisations.
- While 86% of the organisations conduct regular vulnerability testing, 14% do not and that is a risk for them 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. 1% shared that they do not run any security assessments, which is alarming.
- It is good to note that all the surveyed organisations make use of

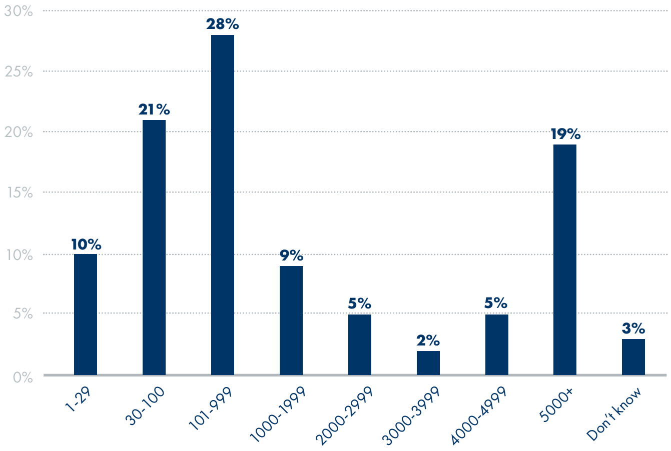
more than one method to protect against malware and ransomware attacks, with anti-malware and anti-virus software being the most used method (78% of the organizations use it).

- User awareness training is one of the methods that most of the organisations (71%) use to detect and respond to phishing attacks.
- Encryption is one of the ways the organisations use to protect sensitive data and information and it is used by 76% of the organisations, followed closely by access controls at 75%.
- 80% of the organisations use access control to detect and respond to insider threats, in conjunction with user monitoring and data loss protection.

DATA ANALYSIS AND INSIGHTS

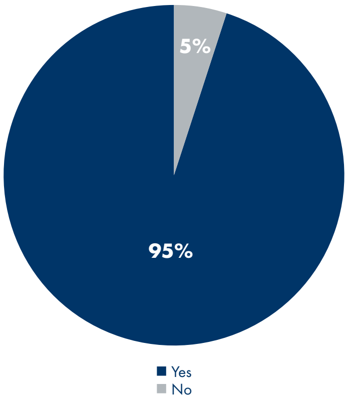
Organisation Size – i.e. the number of employees currently employed at the organisation.

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



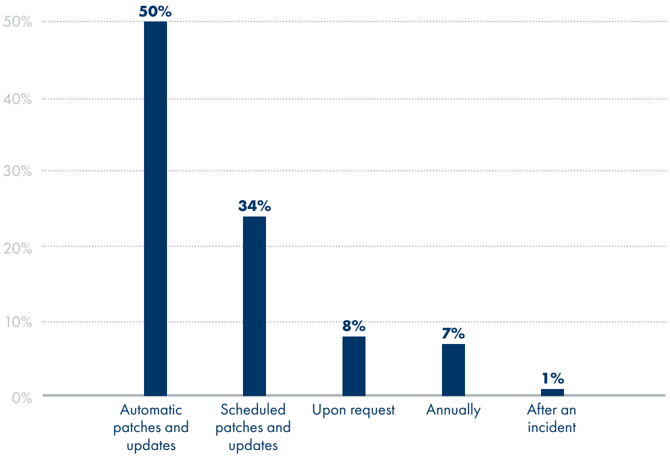
Information Security Policy for Access Management: 95% of organisations do have one.

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



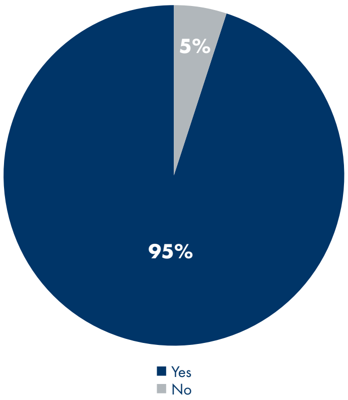
Security Patch and Update Application Frequency: 50% of the organisations perform automatic patches and updates.

» *How often are security pathes and updates applied to your organisation's system?*



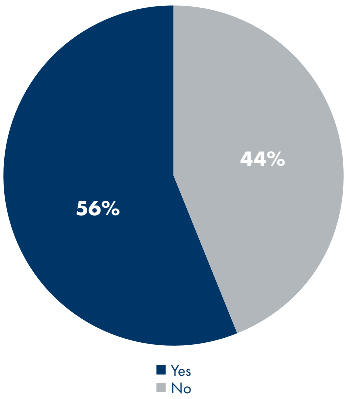
Data Backup and Recovery Plan: 95% of the organisations do have a data backup and recovery plan in place.

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



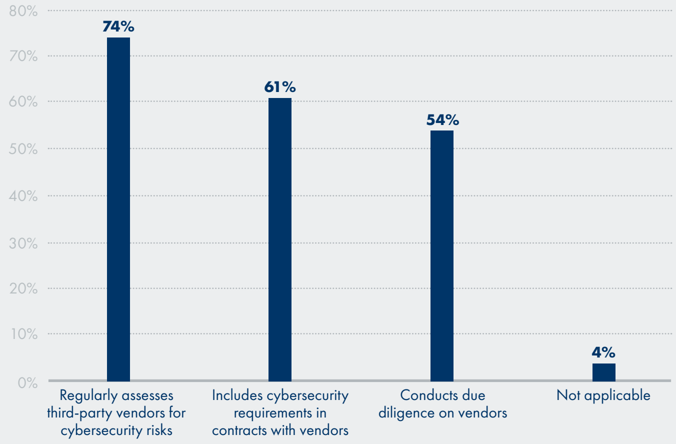
Data Breaches Experienced (Past Year): 56% of the organisations have experienced some data breaches over the past year.

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



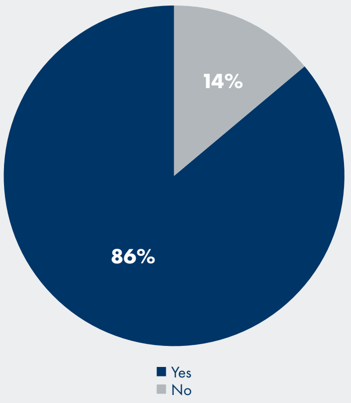
Methods for Identifying and Managing Third-Party Cybersecurity Risks: Amongst other methods, most of the organisations (74%) regularly assess third-party vendors for cybersecurity risks.

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



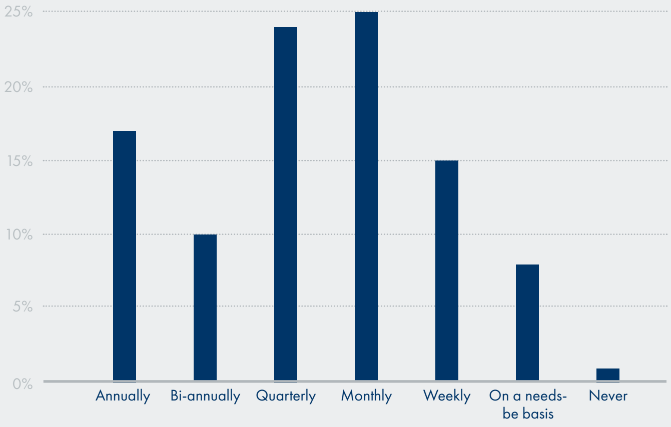
Regular Vulnerability Testing: While 86% of the organisations conduct regular vulnerability testing, 14% do not.

» *Does your organisation conduct vulnerability testing on a regular basis?*



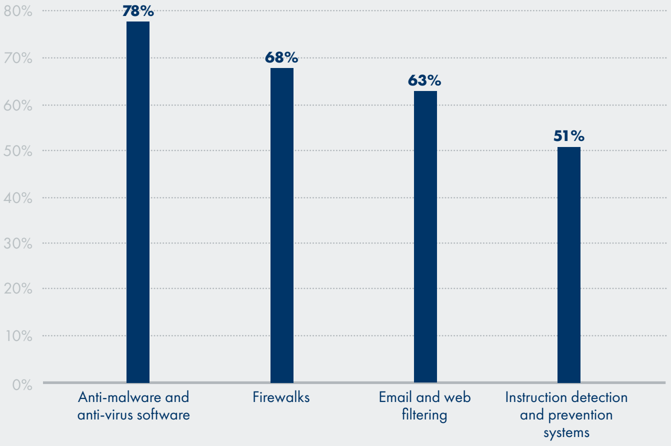
Security Assessment Frequency (Networks and Systems): 25% of the organisations run monthly security assessments on their networks and systems.

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



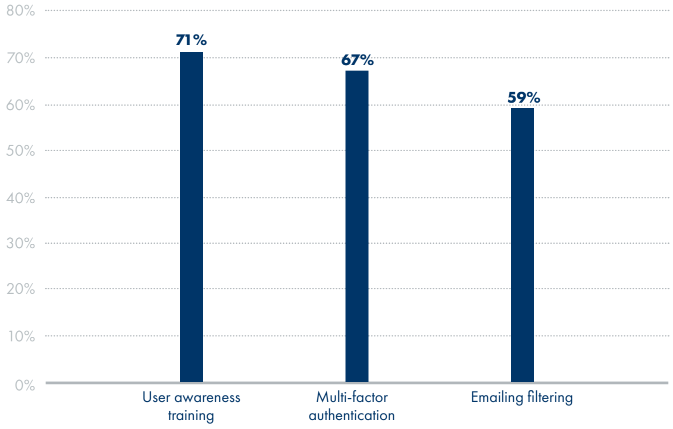
Measures to Protect Against Malware/Ransomware Attacks: Most (78%) of the organisations make use of anti-malware and anti-virus software to protect against malware and ransomware attacks, amongst other measures.

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



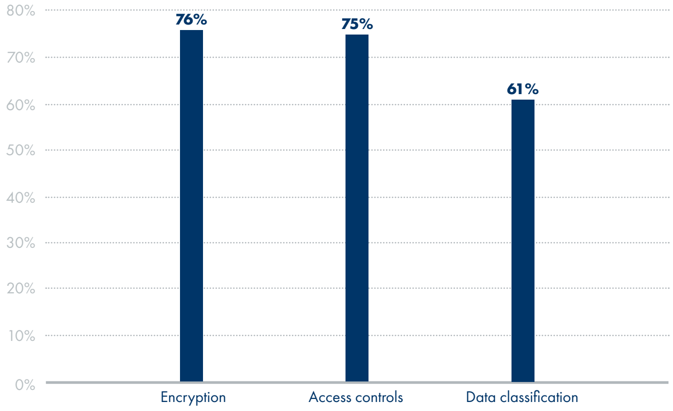
Methods to Detect and Respond to Phishing Attacks: User awareness training is one of the methods that most of the organisations (71%) use to detect and respond to phishing attacks.

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



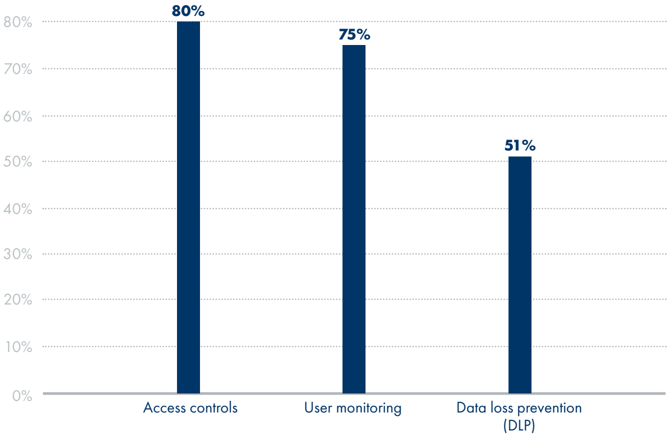
Methods to Protect Sensitive Data and Information: Encryption is used by 76% of the organisations to protect sensitive data and information.

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



Measures to Detect and Respond to Insider Threats: Out of the three measures provided below, 80% of the 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.*



Authors: Zubeida Dawood, Avuya Shibambu, Thuli Mkhwanazi, Oyena Mahlasela, Errol Baloyi, Noku Siphambili

REPORT 3: *COMPLIANCE WITH CYBERSECURITY REGULATIONS*

With the prevalence of cybersecurity attacks, how do public sector organisations ensure their fortification? Are policies really a safeguard? Should we be concerned about public sector cybersecurity posture – or are they at the required frameworks and standards?

Findings from a survey shed some light on methods that organisations employ to make sure they remain compliant and constantly improve their posture.

Key Takeaways:

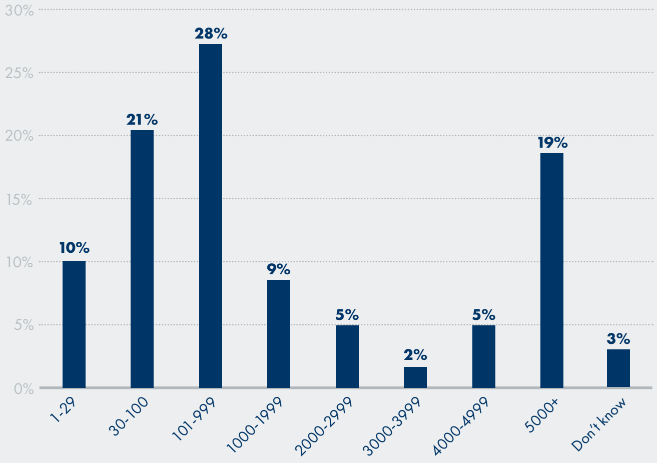
- Organisations surveyed employ various methods to ensure they comply with regulations and standards; 68% of them use the regular assessment of their compliance levels against what is required.
- On the positive, 79% of the organisations perform regular reviews and updates of their cybersecurity policies and procedures.
- Most organisations are aware of the importance of implementing various frameworks and standards; a popular option with 71% of them is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Unfortunately, 5% reported to not be following any cybersecurity frameworks or standards.
- All the organisations review their policies and procedures over various intervals ranging from monthly, quarterly, biannually, and annually. A majority of them (30%) perform the reviews quarterly.
- 43% of the organisations use automated software tools for mapping their cybersecurity controls to available frameworks and standards.
- To gauge their cybersecurity posture against frameworks and standards, 41 % of the organisations conduct regular self-assessments.

- Because cybersecurity is such an important part of running an organisation, it is worthy of sufficient financial investment. Organisations use various methods to invest in cybersecurity and 70% allocate resources based on the risk and maturity levels identified in the frameworks/standards.
- Dealing with a variety of stakeholders, organisations have to show that they adhere to cybersecurity regulations. 65% of the organisations use third-party reports or certificates to this end.
- Once an incident has occurred and has been assessed, it is good practice to incorporate the lessons learned into the organisation's compliance approach. 66% of the organisations perform regular updates of their cybersecurity policies and procedures to incorporate the lessons learned; 44% use it in cybersecurity awareness and training for employees.

DATA ANALYSIS AND INSIGHTS

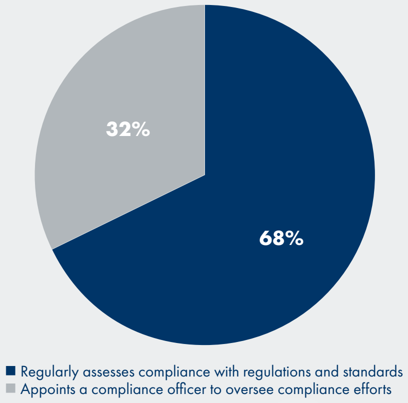
Organisation Size: The number of employees currently employed at the organisation.

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



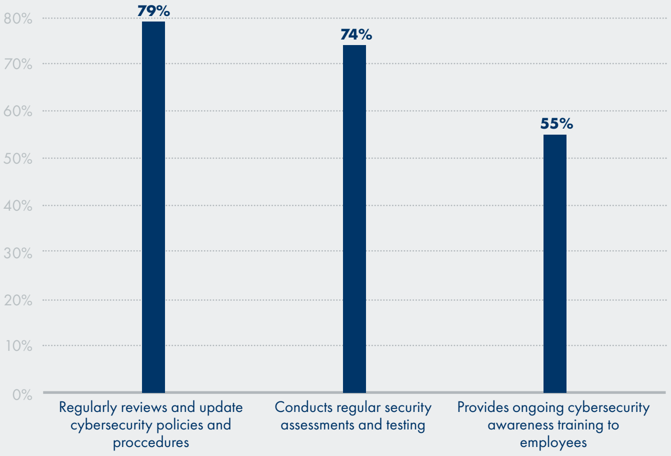
Methods for Ensuring Compliance with Regulations and Standards: 68% of the organisations perform regular compliance assessments with regulations and standards.

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



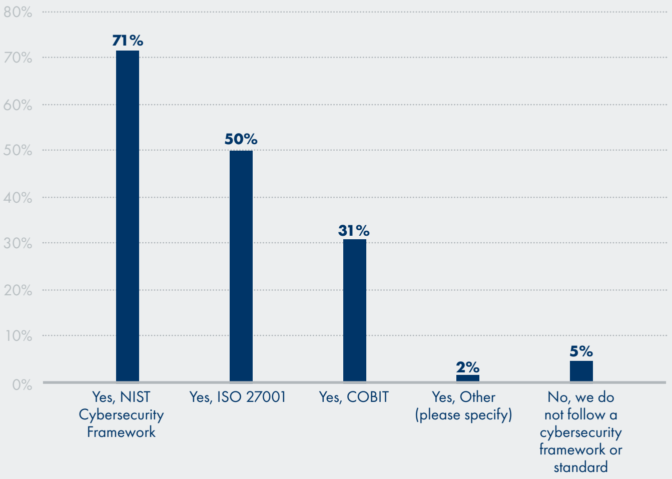
Steps Taken to Improve Cybersecurity Posture: Most of organisations (79%) perform regular reviews and updates of their cybersecurity policies and procedures as part of the steps they take to improve their cybersecurity posture.

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



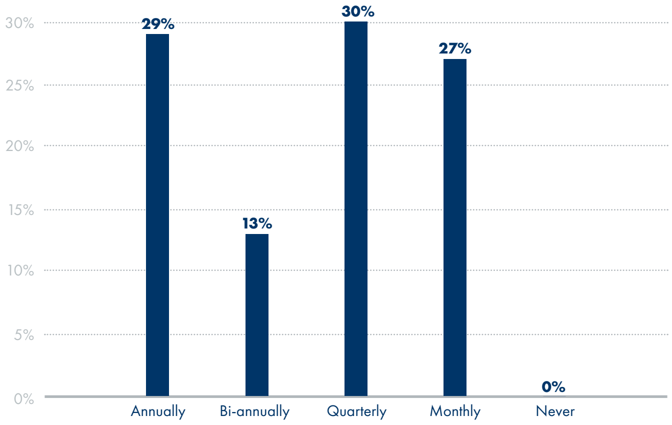
Cybersecurity Frameworks or Standards Followed: 71% of the organisations follow NIST, among other cybersecurity frameworks or standards.

» *Does your organisation follows a cybersecurity framework or standard? Please select all that apply?*



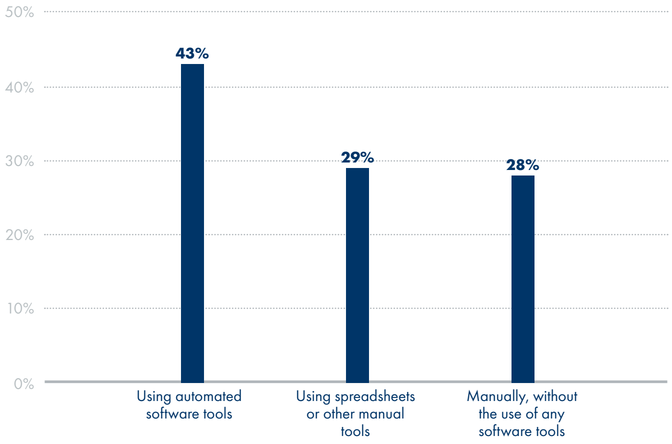
Cybersecurity Policy and Procedure Review Frequency: 30% of the organisations review their cybersecurity policies and procedures quarterly.

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



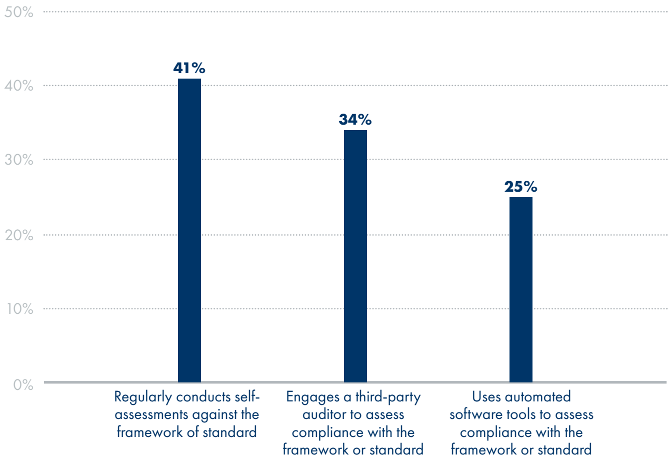
Methods for Mapping Cybersecurity Controls to Frameworks/Standards: 43% of the organisations use automated software tools for mapping their cybersecurity controls to frameworks and standards.

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



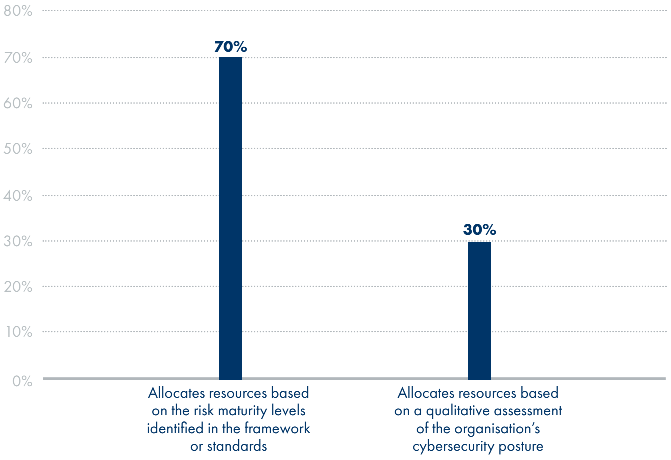
Methods for Measuring Cybersecurity Posture Against Frameworks/Standards: 41% of the organisations regularly conduct self-assessments against frameworks/standards to measure their posture.

» *How does your organisation measure its cybersecurity posture against cybersecurity framework or standards?*



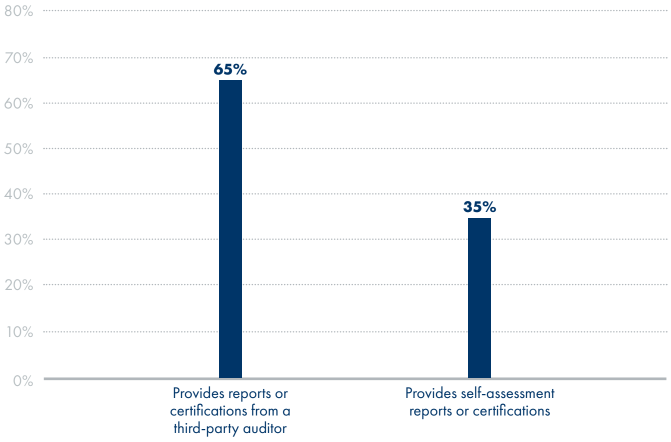
Cybersecurity Investment Prioritization Method: 70% of the organisations allocate resources based on the risk and maturity levels they have identified in the frameworks/standards as their cybersecurity investment prioritization method.

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



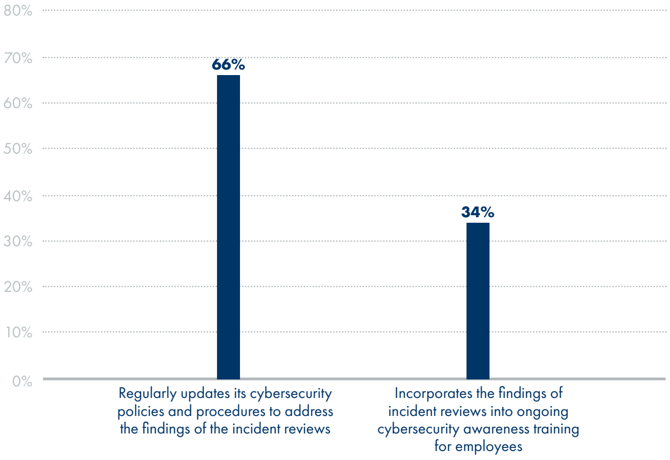
Methods for Demonstrating Compliance to External Stakeholders: 65% of the organisations provide reports or certificates from a third-party auditor to demonstrate compliance to their external stakeholders.

» *How does your organisation demonstrate its compliance with cybersecurity framework standards to external stakeholders?*



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

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



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

CSIR CYBER ARMY – THE NEW 'SECRET SERVICE'

There is an army operating in the shadows. Its members do not march down the streets, fly around in helicopters, or handle weapons on the battlefield. This army chooses to operate behind the scenes; it sits in silence and crawls into the gaps. It is both everywhere and nowhere.

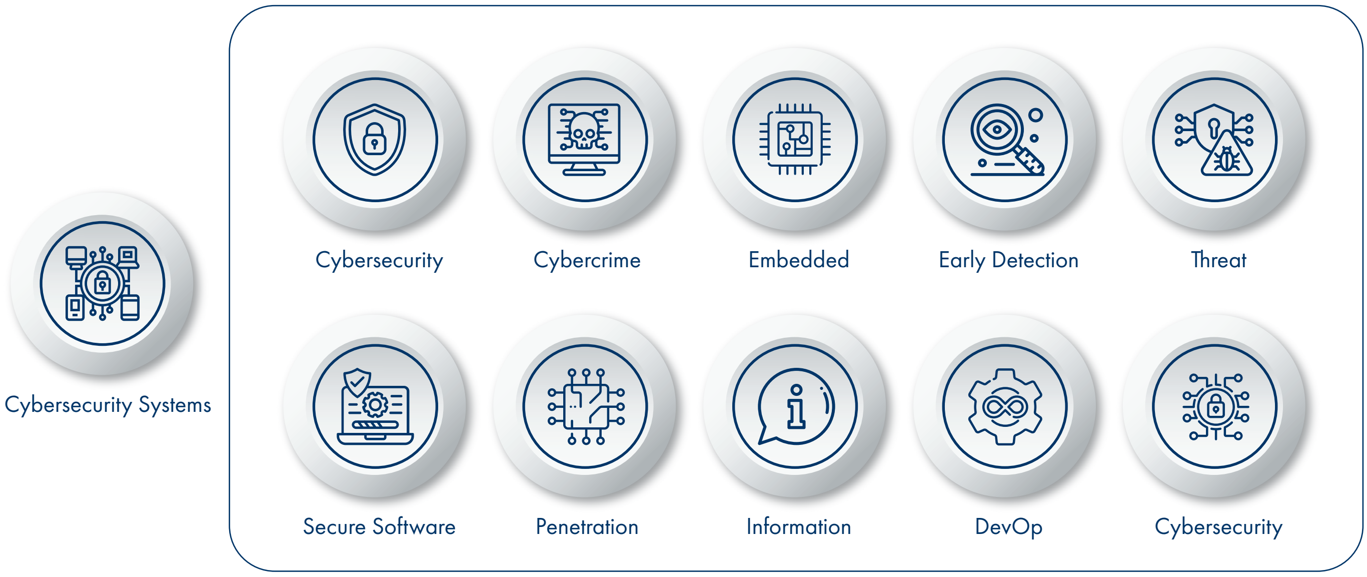
The threats to South Africa and its people are legion and ever-increasing, both from within and from without. This army sees it all. It observes, surveys, plans, formulates, hones its skills and then takes action.

This army is growing, and it does not operate alone. It collaborates with the private sector, the public sector, educational institutions and the South African population as a whole. It works with law enforcement, the military, security agencies, universities, small local businesses and well-established private organisations. The army realises that it cannot operate alone, and that is its strength. It is up to everyone to secure and protect the country. There exists the shared, inescapable mandate to equip ourselves with the knowledge and skill to defend ourselves.

The army's reach and mandate are vast, covering cyberwarfare, cybercrime investigations and cybersecurity. It has its work cut out. This army hacks, cracks, breaks, builds, develops, supports and enables. It is cutting-edge. It breaks into systems to secure them, cracks software to exploit it and reverse engineer it, and builds in-house tools to help defend and penetrate. It follows the evidence to help track down perpetrators. It is both offensive and defensive while maintaining a strategic focus. It gathers, develops and shares knowledge to expand its own capabilities and those of others.

If it connects to a network, runs software or exists in cyberspace, this army is equipped to handle it.

This army is the Cybersecurity Systems research group, which consists of several cybersecurity specialists, software developers, engineers, computer scientists and researchers. They are involved in technical aspects of cybersecurity, cybercrime investigation and cyber warfare within the CSIR Information and Cybersecurity Research Centre. They work with us, for us and represent us all.



YOUR IDENTITY IS **ON THE LINE**

In an age when lives and businesses are run in cyberspace, efficient identity management has become paramount. The CSIR's Secure Identity Systems research group is at the forefront of interventions to ensure and protect national identity-driven information security systems and infrastructure.

The CSIR dedicates itself to the national imperatives of building a capable state, ensuring the safety of citizens and communities, and contributing to the development of reliable and robust social and economic infrastructure. The primary focus of the Secure Identity Systems group is tackling technological challenges and delivering research, development and innovation interventions for identity authentication mechanisms that underpin service delivery, prevent crime and support personal and national security.

With identity-driven systems dominating the way people operate, robust authentication technologies are needed to safeguard online activity, protect identities and prevent fraud and theft.

Protection on one side of the coin and effective detection on the other: Strong identity management capabilities allow authorities to track criminals more efficiently, reducing unauthorised immigration and its associated security threats.

CASE STUDY: ACCESS TO SOCIAL GRANTS

South Africa integrates social services and financial inclusion to enhance the lives of its citizens. People with a secure and verifiable identity can access financial services such as bank accounts and credit, thus contributing to the economy. However, some challenges in the social services sector require expert intervention.

For instance, grant payment systems rely on fingerprints to link each client to a unique identity. The fingerprints of new grant applicants are compared against those of existing clients. A grant application is only processed after determining that the applicant's prints do not match those of any other client in the system.

This is in response to past identity-based social grant fraud, where one person succeeded in applying for more than one social grant using different identities, and multiple people applied for child support grants for the same child using different identities. However, challenges arise in comparing fingerprints, particularly with children, as existing fingerprint scanners have difficulty capturing good-quality fingerprints, especially those of newborns and infants. The prevalence of fraudulent payouts will only be solved with technology capable of capturing infant biometric characteristics.

WHY *"IDENTITY FROM THE CRADLE TO THE GRAVE"* IS OUR MANTRA

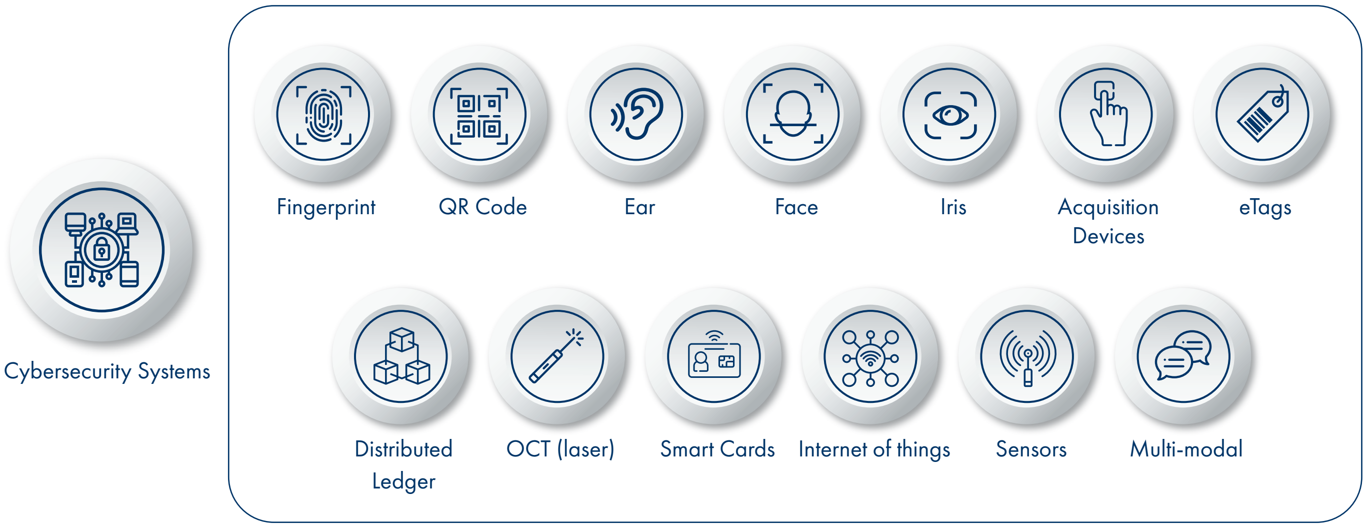
The CSIR develops biometric-based technologies that can be deployed to a myriad of applications, including access control, registration of individuals for provision of services and improvement of identification of children or minors. The group has created multimodal biometrics systems and multifactor authentication platforms to counter cyber attacks on identity systems. In addition to working with individuals, they also focus on livestock identification and traceability systems.

The CSIR has also developed technology to read the biometric measurements of cadavers by detecting subdermal minutia. Currently in use at selected government morgues, the technology assists in dealing with a backlog of unclaimed deceased individuals.

Furthermore, with the rapid digitisation of consumers' lives and enterprise records, along with the associated risk of breaches, the CSIR is developing decentralised digital identity systems that can be used across enterprises. This would limit data exposure to cyber attacks and give users control over their data.

The team comprises experts in software development, systems engineering and machine learning, which allows for data science and analytics capabilities across various socioeconomic sectors.

Contact:
RETHABILE KHUTLANG,
Research Group Leader
Secure Identity Systems
+2773 852 3559
rkhutlang@csir.co.za



Cybersecurity Systems

Fingerprint

QR Code

Ear

Face

Iris

Acquisition Devices

eTags

Distributed Ledger

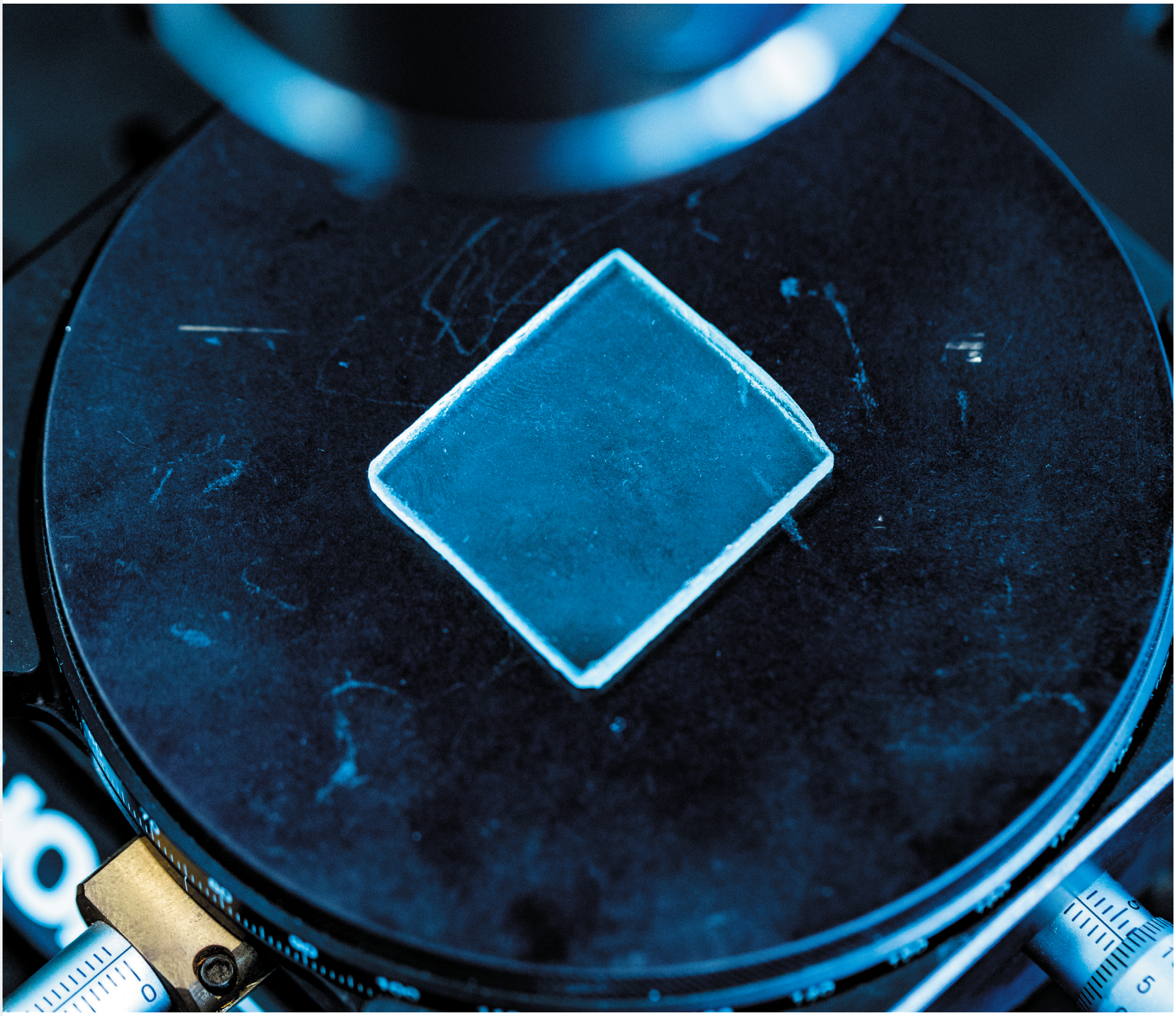
OCT (laser)

Smart Cards

Internet of things

Sensors

Multi-modal



COLLABORATION IN CYBERSECURITY

The CSIR places great emphasis on collaboration and partnerships. The CSIR Information and Cybersecurity Centre pursues partnerships with the private sector (for technology commercialisation projects), higher institutions of learning (for collaborative research) and government (for policy implementations). The collaborations are intended to build capacity, capabilities and a sustainable knowledge-based national workforce that support the needs of government, industry, and academia.

HIGHER EDUCATION INSTITUTIONS: THE UNIVEN EXAMPLE

In line with the role that the CSIR plays in the National System of Innovation, the Centre collaborates with several higher education institutions in South Africa. At the advent of each financial year, specific institutions are selected for engagement.

In 2024 the focus was on the University of Venda (Univen), Tshwane University of Technology (TUT) and Nelson Mandela University (NMU).

In the case of Univen, a Memorandum of Understanding (MoU) was signed previously, in 2020 and a structured implementation plan, with work packages, tasks, and activities for technical leaders was put in place.

Use as caption: The CSIR/Univen MoU Steering Committee had its second physical meeting at the University of Venda in April 2024. The University's Faculty of Management, Commerce and Law hosted Dr Jackie Phahlamohlaka from the CSIR for a guest lecture on national cybersecurity issues.

CSIR cyber experts also presented on Livestock Identification and Traceability, infant biometrics (fingerprints, irises and outer ear pattern) as well as the Cybersecurity Learning Factory which provides modular and hands-on experiential training.

> In the words of the Executive Dean of the Faculty of Management, Commerce and Law, Prof Barwa Kanyane; *"through the collaborative efforts of CSIR and UNIVEN, we are poised to make significant strides in addressing the myriad challenges posed by cybersecurity in today's ever-evolving digital landscape."*
>
> – Univen News, 15 April 2024)

Two Univen students were quick to express interest to pursue their PhD studies in Cybersecurity.

Contact: Dr Jackie Phahlamohlaka
JPhahlamohlaka@csir.co.za

Dr Jackie Phahlamohlaka

SELECTED RESEARCHERS

ICSC RESEARCHERS PROFILES

Researcher Profile:

Dr NNP Mkuzangwe

Dr Nenekazi holds a PhD in electrical and electronic engineering from the University of Johannesburg and an MSc in mathematical statistics from Rhodes University. She obtained her first degree in 2001. She has taught mathematical statistics/statistics to science, commerce and health science students at Nelson Mandela University. Nenekazi joined the CSIR in August 2013 under a PhD Studentship Programme and was permanently employed as a network and data security researcher in January 2018. In July 2020, Nenekazi joined the CSIR's Data Security and Analytics research group.

Research Interests: Predictive modelling, intrusion detection, data security/privacy

Masters Students:

4. Currently mentoring Hombakazi Ngenjane. Digital Forensics Supported by Machine Learning for the Detection of Online Sexual Predatory Chats.

She has mentored university students in applying statistics-based machine learning techniques to analyse real-life data to inform decision-making in a project called "Data Science for Impact and Decision Enablement," sponsored by the Department of Science and Innovation. She has reviewed an international journal article in the field of intrusion detection.

Researcher Profile:

Dr Moses Dlamini

Dr Moses Dlamini is a senior researcher with a focus on information security, cybersecurity, cloud computing security, security of the internet of things, securing artificial intelligence and machine learning classification models, security of operational technology and industrial control systems, securing industry 4.0, digital deception, context-aware and behavioural authentication, privileged access management, identity and access management, conflict-aware access control, digital forensics and chaos-based cryptography.

Dlamini publishes his research work both in both national and international forums. He is also a reviewer of several information security and privacy journals and conferences. He is passionate about technology that serves the needs of society and industry.

He holds a PhD in computer science (2020), an MSc in computer science (2010) and a BSc Hons. in computer science (2007), all from the University of Pretoria. He also obtained a BSc in computer science and mathematics from the University of Swaziland (2002)

Research Interests: Information and cyber security analytics, detection and prevention of adversarial artificial intelligence and machine learning attacks, design of future-proof and zero-trust cybersecurity architectures, detection of digital deception and fourth industrial revolution security. Cybersecurity governance, cybersecurity culture, security awareness, training and education.

Researcher Profile:

Sipho Ngobeni

Sipho Ngobeni is a senior researcher and plays a leading role in assisting industry and government in developing and implementing cybersecurity governance instruments (strategies, policies, processes, procedures, frameworks and standards), cybersecurity assessments, security configuration reviews, threat modelling and operationalising computer security incident response teams. He has authored and co-authored numerous peer-reviewed papers.

Ngobeni holds an MSc in computer science from the University of Pretoria (2016), a BSc Hons. in computer science from the University of Zululand (2007) and a BSc in computer science from the University of Zululand (2006).

Research Interests: Cybersecurity governance, cybersecurity assessments and audits, data privacy and protection, digital forensics and security operations.

Researcher profile:

Rethabile Khutlang

Rethabile Khutlang's interests are biological image analysis, exemplar and latent fingerprint acquisition and 3D image analysis using optical coherence tomography. Khutlang has a master's degree in biomedical engineering from the University of Cape Town. His experience at the CSIR includes working as a biological and biometrics engineer. Khutlang leads teams working on embedded tokens, data analytics platforms, fingerprint analysis software development kits and a biometrics suite platform. He also leads a team using OCT to address fingerprint spoofing, usage of fingerprints inside skin and lifting fingerprints none destructively from crime scenes.

Research interests: Image processing, machine learning, biometrics and data analysis

Researcher profile:

Dr Namosha Veerasamy

Dr Namosha Veerasamy is a senior cybersecurity researcher with a demonstrated history of working in the research industry. She is skilled in management, networking, security, cyber awareness, and cyber defence.

Her qualifications include a BSc in it computer science, a BSc Hons. in computer science (Honours), an MSc in computer science (with distinction) and a PhD in Computer Science. She is also a Certified Information System Security Professional (CISSP) and a Certified Information Security Manager (CISM).

Research interests: Financial technology threats, cybersecurity policy, cybersecurity skills assessment, cybersecurity awareness creation and the knowledge of cyber threats.

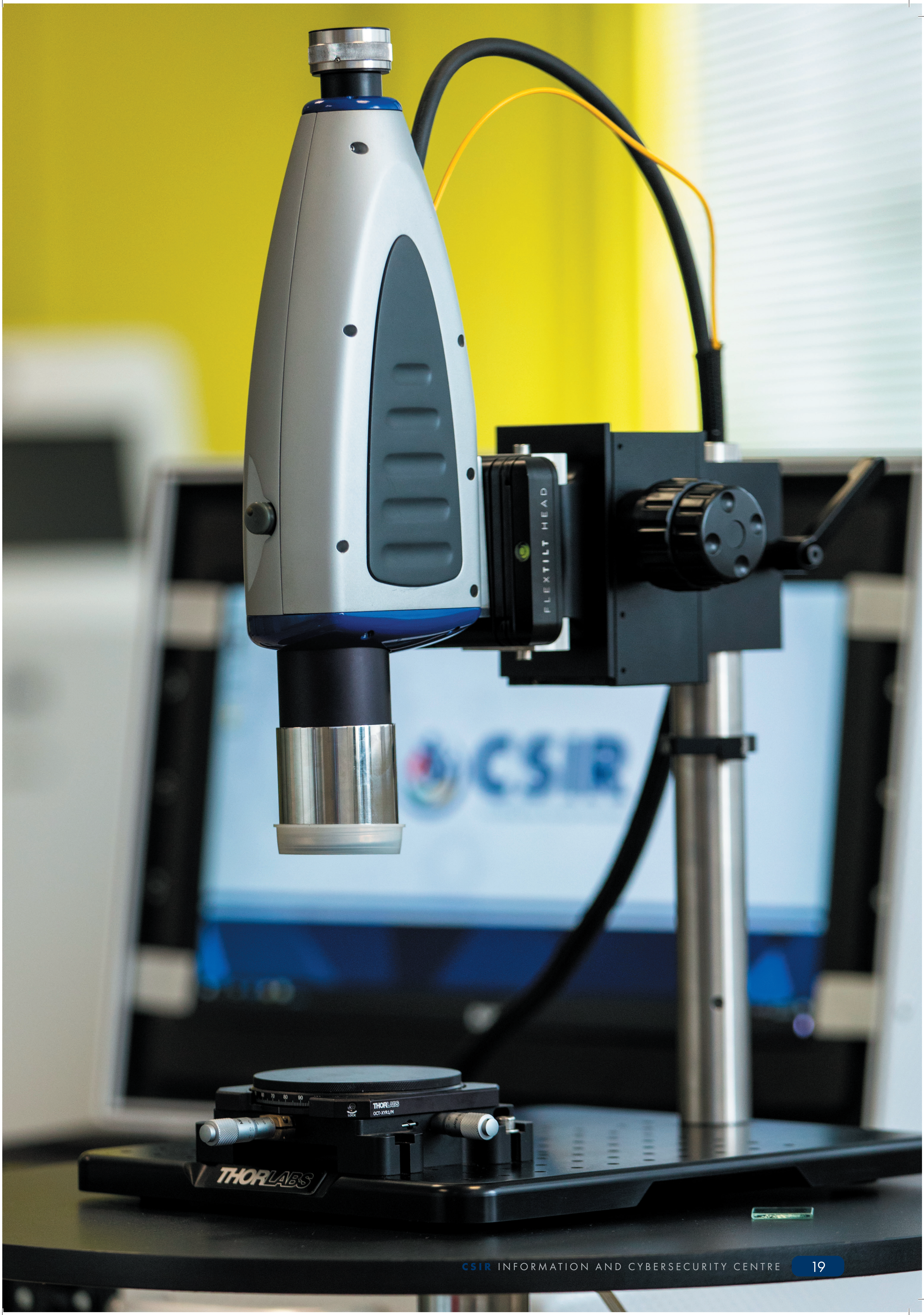
Researcher profile:

Dr Andre Mcdonald

Dr Andre McDonald is an experienced technology specialist with a demonstrated history of working in the research industry—a strong professional skilled in dynamical systems, chaos theory, signal processing, information theory and cybersecurity.

He holds a BEng in Computer Engineering, a BEng Hons. and a MEng in electronic engineering.

Research interests: Dynamical systems, chaos theory, signal processing, information theory and cybersecurity.


FLEXTILT HEAD
CSIR
THORLABS
OCT-XYR1/M
LOCK
THORLABS

DO YOU HAVE WHAT IT TAKES TO BE A CYBER WARRIOR?

Grabbing the phone, squinting to read the screen, it says caller ID Vhuthu.... Vuthu?? At 04:00 in the morning?? The dude from ICT??

MINUTES LATER...having flewn out of bed, rushed through a shower, you head for the office. No time for coffee. From what Vhuthu said, this was going to be a tough day....

....but where do you even start? When you arrive they will expect you to give guidance.

All those years working in IT, all those clever papers and articles on cybersecurity you impressed everyone with – comes down to this. This day. This challenge. Millions depending on it.

All systems and applications are down; even the backups are inaccessible.

One single computer system or application not being available is one thing, because there are backups, but ransomware. Ransomware, well, that is different, isn't it? The organisation has received a ransom note that the backup administrators saw on one of the servers – and then lost total control of all the servers.

What do you tell the Department when they wake up with no computer systems? How long will it take to recover? What is the impact? What is the cost? How do you go about giving guidance?

THE HARSH REALITY

In reality – according to PWC Global CEO survey report of 2024 – cyber risks are the third major risk faced by businesses. In context, cyber risks to organisations are only behind inflation and macroeconomic volatility, but ahead of geopolitical conflict, climate change, health risks, and social inequality.

In South Africa, the increasing trend in data breaches is also observed through breach notifications to the Information Regulator. By June 2023, the Information Regulator in South Africa had received over 1 021 cyber data breach notifications - double the number that was reported in the previous five months of the same year

With the scope and depth of capabilities at the CSIR Information and Cyber Security Centre, urgent calls in the middle of the night are not unusual as they are called upon to assist with a number of cybersecurity incident responses across South Africa every year.

Systems engineers, cybersecurity researchers, analysts and cybersecurity engineers operate in the Virtual Security Operations Centre to prevent or manage critical cybersecurity threats – in real time – with virtually 24/7 Endpoint Detection and Response, Security Orchestration, Automation and Response and SIEM - Security Information and Event Management.

Who are you going to call? Our capabilities include:

- Guidance and hands-on support on cybersecurity incident response.
- Incident Management according to NIST SP 800-61.
- Governance, risk and compliance such as policies, procedures, quantitative risk assessments (penetration testing and vulnerability assessment) and qualitative risk assessments (survey questions to system administrators).
- 24x7x365 Managed Security Operations Centre according to NIST SP 800-137.
- Awareness training for employees, and contractors.
- Digital Forensics investigations for computers, servers, mobile phone, emails, and report generation for court cases.
- Security tool administration (firewalls, load balancers, internet proxy, email gateway, SIEM tool, SOAR tool, Endpoint Detection & Response, and so on).
- On-call for certified Senior Cybersecurity Professionals.
- Human Capital Development on the above services.

Sources:
PWC report *https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey.html*
Information regulator numbers: [https://www.itweb.co.za/content/j5alrMQAJOQMpYQk].

Muyowa Mutemwa
Research Group Leader: Data Security & Analytics
MMutemwa@csir.co.za

SPECIAL SURVEY REPORT

DATA BREACHES IN SOUTH AFRICA: MALWARE, MALICIOUS ACTORS AND MORE

As security breaches continue to escalate, security professionals urgently require actionable data to make informed decisions for their organisations. The CSIR Information and Cybersecurity Centre conducted a national survey, drawing 309 respondents from various provinces, including officials from diverse sectors, such as public, private, non-profit and small, medium and micro enterprises (SMMEs). Participants held positions as executives, directors, managers, or contributors in fields like information technology, cybersecurity, software development and development operations, with direct or indirect responsibility for cybersecurity within their organisations.

The objective of the survey was to provide a detailed overview of the cyberattack landscape facing South African organisations. The survey probed issues such as how organisations are breached, the initial causes of attacks, resolution times and the financial impact associated with these incidents. Ultimately, the aim was to determine ways of assisting security professionals and leaders in developing well-informed, strategic responses to cyber incidents.

This report presents data analysis and key insights based on the types of cyberattacks experienced, methods used, impact on the information technology infrastructure and techniques used to mitigate, prevent or remediate these attacks.

DATA ANALYSIS AND KEY FINDINGS

Frequency of breaches over 12 months

About 88% of the participants admitted having suffered a security breach during the past 12 months (see Figure 1), and of this group, 90% were targeted multiple times. This can imply that a successful initial attack increases the likelihood of subsequent attacks on the same organisation's infrastructure.

Those who reported "none" did not mention their preventative, mitigation and remediation measures compared to those who had been compromised. These organisations may either be exceptionally secure or possibly unaware of events occurring. In future surveys, it might be useful to ask if new activities or systems were implemented as a direct result of a specific or series of breaches.

» *Number of breaches over the last 12*

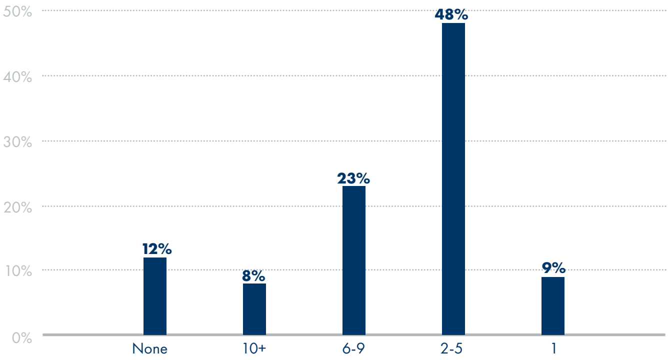


Figure 1: Number of incidents experienced in the past 12 months

Types of cyber breaches experienced

As shown in Figure 2, the top three cyberattacks facing organisations were malware (65%), which is the most commonly mentioned, with just over half (55%) reporting application attacks and third experienced insider threats (30%). Other attacks reported by less than 30% included crypto-jacking or crypto-mining, wiper attacks and ransomware. The lowest number of incidents (8%) were out down to DDos. In a nutshell, almost 87.8% of the organisations experienced at least one type of cyber incident in the past 12 months, and one-third (35.3%) had experienced three or more incidents.

» *Types of cyberattacks experienced*

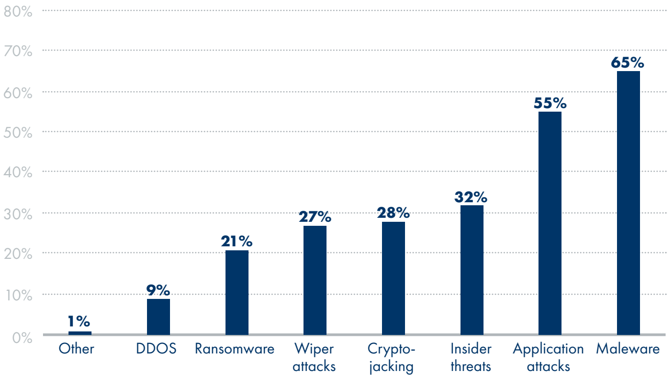


Figure 2: Types of cyberattacks experienced

Root cause

A popular root cause was third-party connected to the enterprise at (48%), with similar proportions stating it was phishing (45%) or hardware-based attacks (43.0%), as shown in Figure 3. Less frequently mentioned causes were supply chain attacks through SaaS, DevOps Depos (e.g. GitHub), and the least (9%) reported IOT. Organisations gave different root causes – or even more than one reason for the same attack. It was not possible to link the cause with the type of attack where more than one was mentioned.

» *Source of the breach*

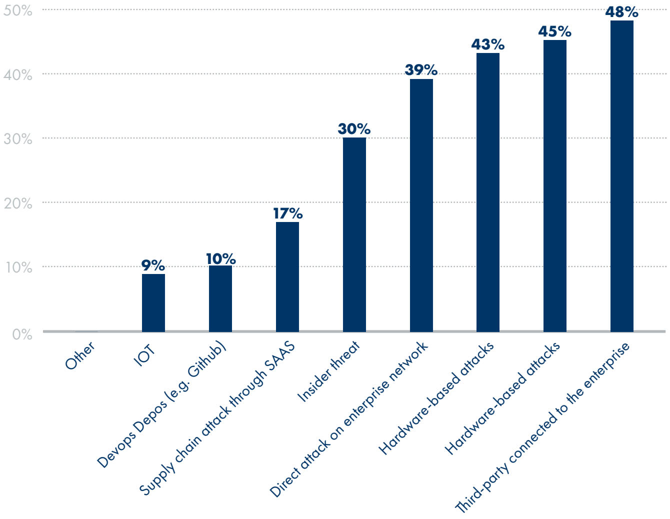


Figure 3: Source of the cyberattack

Impact

The study sought to understand the impact of the attacks, including damage to infrastructure, financial loss, the time it took for the organisation to resolve the issue and data loss – particularly personal Identifiable information (PII). Overall, three-quarters reported a low to moderate impact (78%), with only 4% reporting a very high impact, as shown in Figure 4**.** Although it was not possible to link the exact type of incident with impact, it was noted that fewer incidents were related to a lower impact. However, some organisations mentioned that in some cases, only one event caused a very high impact.

» *Overall impact per frequency of the attack*

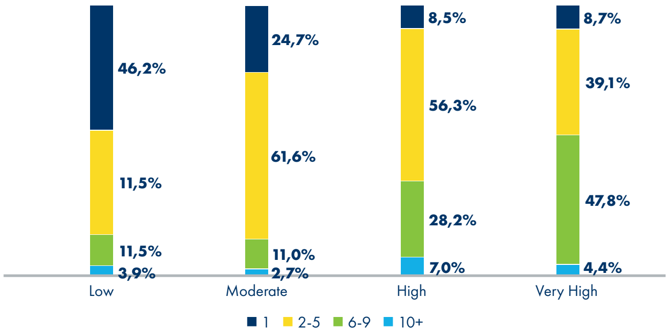


Figure 4: Overall Impact of cyber-incidents on organisations

Recovery

Figure 5 shows that the majority of low-impact incidents took hours to resolve, but this proportion was reduced by almost half to 45.5% in cases of high impact. Over a quarter of organisations reported time for recovery in very high-impact circumstances in a measure of months. Such respondents also had commonly experienced denial of service attacks.

» *Overall impact per frequency of the attack*

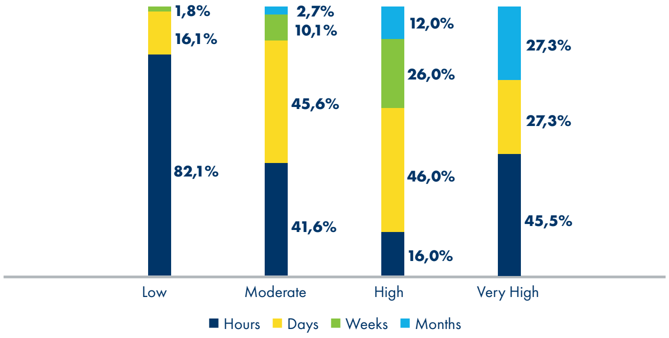


Figure 5: Recovery time according to the impact of an incident

Financial loss

The monetary value incurred due to the attack was correlated with the disruption caused to the organisation (i.e. shorter disruptions generally incurred lower costs), with only (3%) incurring over a million rands as a result of the breach, Figure 6. However, there were exceptions where brief disruptions resulted in substantial expenses. Financial loss could have been influenced by other factors such as fines, hiring service providers, or loss of business profits due to the disruption.

» *Financial Cost*

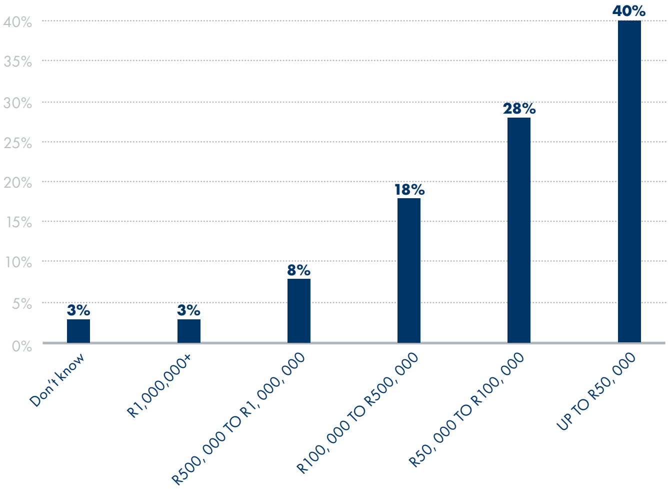


Figure 6: Financial Cost

Data loss

Lastly, on impact, Figure 7 shows that about (42%) experienced data loss, particularly PII records, due to the attack, while the rest (58) indicated that the impact of the attack did not result in any loss of such records.

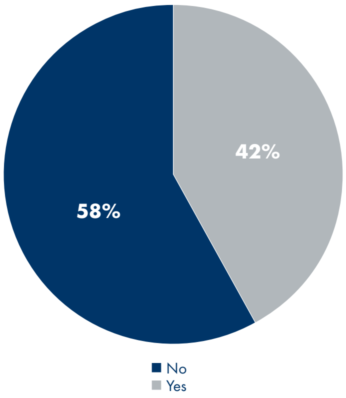


Figure 7: Data loss (PII) due to cyberattack

Contact:
Homba Ngejane
hngejane@csir.co.za

CONTACTS

DR JABU MTSWENI

Head of the Information and Cyber Security Centre
JMtsweni@csir.co.za
+27 12 841 4394

DR MOSES DLAMINI

Research Group Leader (Acting): Governance, Privacy and Trust
tdlamini1@csir.co.za
+27 12 841 5018

BILLY PETZER

Research Group Leader: Cybersecurity Systems
bpetzer@csir.co.za
012 841 7313

RETHABILE KHUTLANG

Research Group Leader
rkhutlang@csir.co.za
012 841 2257

MUYOWA MUTEMWA

Research Group Leader
mmutemwa@csir.co.za
012 842 7326

CSIR
Touching lives through innovation