January 2025

Inaugural Annual Cybersecurity Indaba 2024 Report

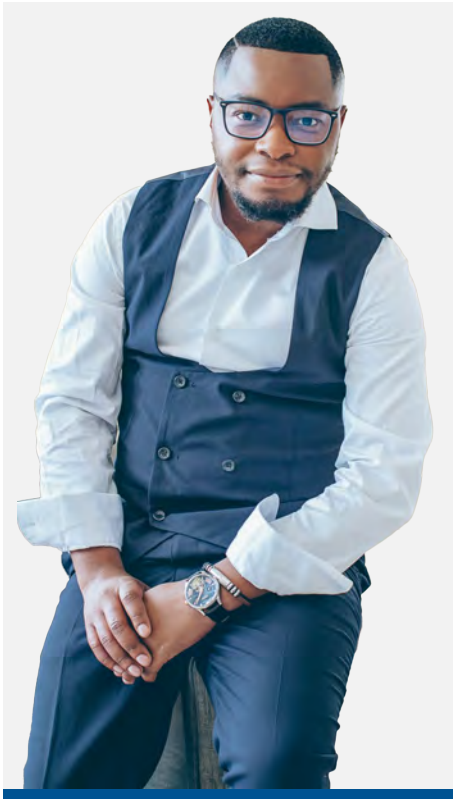
Safeguarding South Africa's Digital Future

Prepared by

cyberm

Table of Contents

1. Foreword by the Chief Empowerment Officer of CyberM8



Thabang Phala
CEO: CyberM8 Initiative NPC

The **Inaugural Annual Cybersecurity Indaba 2024** marks a significant milestone in South Africa's ongoing efforts to build a resilient digital ecosystem. In an era where cyber threats are evolving at an unprecedented rate, fostering collaboration among government, private sector, academia, and civil society is more critical than ever. This Indaba served as a vital platform for stakeholders to share insights, identify solutions, and commit to proactive cybersecurity measures.

As the Chief Empowerment Officer of **CyberM8**, I am proud to have witnessed the collective dedication displayed by participants, speakers, and partners. The Indaba underscored the importance of knowledge sharing, skills development, and strategic partnerships in strengthening our national cybersecurity posture. The insights gathered from the survey responses, discussions, and expert panels provide a strong foundation upon which we can build robust cybersecurity initiatives for the future.

This report highlights the key discussions, survey findings, and actionable recommendations that emerged from the Indaba. We invite all stakeholders to join us in the journey toward a safer digital South Africa.

2. Executive Summary

The **Inaugural Annual Cybersecurity Indaba 2024** brought together industry leaders, government representatives, cybersecurity professionals, and academics to discuss South Africa's cybersecurity landscape and identify solutions to mitigate risks. The event aimed to address key cybersecurity challenges, enhance skills development, promote public-private partnerships, and advocate for strengthened regulatory frameworks.

Survey responses collected during the Indaba provided valuable insights into the most pressing cybersecurity concerns. Key findings revealed that:

1. **Top cybersecurity challenges** include lack of resources, database breaches, compromised customer data, phishing attacks, and identity fraud.
2. **Most vulnerable sectors** identified were government, finance, healthcare, and SMEs, which often lack the necessary Cybersecurity Professionals and cybersecurity infrastructure.
3. **Emerging technologies** such as AI, IoT, encryption, and automated vulnerability assessments should be prioritised for cybersecurity defences.
4. **Public-private collaboration** can be enhanced through improved information sharing, local threat intelligence, and stricter access control measures.
5. **Educational institutions** play a crucial role in closing the cybersecurity skills gap through early education, practical training programmes, and research initiatives.
6. **Regulatory measures** need stronger enforcement, data privacy enhancements, and increased investment in cybersecurity infrastructure.

This report presents a comprehensive overview of the Indaba's key discussions and survey findings, providing actionable recommendations to drive cybersecurity resilience in South Africa.

3. Overview of the Cybersecurity Indaba 2024

Background and Objectives

The **Cybersecurity Indaba 2024**, hosted by **CyberM8**, was designed to address South Africa's cybersecurity challenges and foster a culture of proactive digital security. The event focused on:

1. Strengthening cybersecurity policies and regulations.
2. Enhancing collaboration between government and the private sector.
3. Bridging the cybersecurity skills gap through training and education.
4. Promoting the adoption of emerging technologies to safeguard digital assets.

Key Themes and Discussions

The Indaba featured expert-led panels and keynote presentations on topics such as:

- **Cyber Threat Landscape in South Africa:** Insights into emerging threats and vulnerabilities across sectors.
- **The Role of AI and Automation in Cybersecurity:** How AI-driven solutions can enhance threat detection and response.
- **Public-Private Partnerships for Cyber Resilience:** Strategies for fostering cooperation between industries and government bodies.
- **Cybersecurity Skills Development and Capacity Building:** The importance of training and education in bridging the skills gap.
- **Regulatory Compliance and Policy Enforcement:** Strengthening national frameworks to ensure cyber resilience.

Official Event Livestream Video:
https://www.youtube.com/live/KCB1oLnxXTc?si=8DoD3YvrvHeLDlt0

Purpose of the Indaba by the CEO:
https://youtu.be/iueDeGPrw7Q?si=lORQgRpG2MOK2i52

4. Cybersecurity Indaba 2024 Partners

5. Event Programme Overview

The **Cybersecurity Indaba 2024** provided a platform for insightful discussions, expert presentations, and networking opportunities. The morning session set the stage with an opening address by Thabang Phala from CyberM8 Initiative, followed by a presentation on *Secure by Design* by Tiyani Nghonyama of Geekulcha. The keynote address by **Molehe Wesi** from **.ZADNA** explored *Envisioning South Africa's Digital Future*, providing a vision for national cyber resilience.

Panel discussions brought together experts from various sectors, including **Neil Dundas** (ZA Registry Consortium), **Prof. Elmarie Kritzinger** (UNISA & CyberAware), **Sipho Mtombeni** (Google South Africa), **Charmaine Strydom** (Absa), **Prof. Sizwe Snail** (Nelson Mandela University), and **David Moepeng** (African Cybersmart Network). These discussions tackled critical topics such as *Safeguarding Our Cyber Ecosystem* and *Building Resilience in Key Industries*. A notable presentation by Neil Dundas from ZA Registry Consortium addressed strategies for combating DNS abuse.

Additional key presentations were delivered by **Thulani Mabuza** from Orange Cyberdefense, who discussed *Unmasking Digital Footprints: Leveraging OSINT for Proactive Cyber Defense*, and **Wayne Poggenpoel** from TFL Consulting, who facilitated an industry-focused panel discussion on strengthening cyber defences.

The afternoon session featured an in-depth presentation by **Steve Jump** from SLVA Cybersecurity, followed by an interactive Q&A session, where participants engaged with experts on pressing cybersecurity challenges. The event concluded with *Indaba Resolutions and the Way Forward*, presented by **Manqoba Mngomezulu**, Chief Operations Officer (COO) of CyberM8, summarising key takeaways and future steps. The Indaba closed with a networking session, fostering collaboration among industry professionals, policymakers, and academics.

This structured programme ensured a comprehensive exploration of South Africa's cybersecurity landscape, equipping participants with actionable insights to enhance national cybersecurity resilience.

6. Attendees Profile

The **Cybersecurity Indaba 2024** attracted a diverse range of participants from across South Africa's cybersecurity ecosystem. Attendees included professionals from government, private sector, academia, and civil society, all dedicated to strengthening national cybersecurity resilience. The event provided a platform for meaningful discussions, knowledge exchange, and networking among key stakeholders.

A breakdown of the attendees is as follows:

- **Cybersecurity Professionals:** Analysts, security engineers, and risk management specialists from various industries.
- **Corporate Executives:** Directors and managers responsible for implementing cybersecurity strategies within their organisations).
- **Academics and Students:** University researchers and learners interested in pursuing careers in cybersecurity.
- **Government Officials:** Representatives from regulatory bodies and policy institutions working on national cybersecurity frameworks.
- **Technology Entrepreneurs:** Start-up founders and SMEs focused on developing innovative cybersecurity solutions.

The turnout of academics and students highlights a growing interest in cybersecurity education, which aligns with the Indaba's focus on skills development and capacity building. Meanwhile, corporate executives and cybersecurity professionals brought industry insights that contributed to discussions on emerging cyber threats and risk management strategies.

7. Contributors and Speakers

The success of the Indaba was driven by contributions from esteemed speakers and experts in the cybersecurity industry. The event featured insights from:

- **Government Representatives:** Cybersecurity policymakers and regulatory bodies shared updates on South Africa's national cybersecurity strategy.
- **Industry Leaders:** Experts from major technology companies, financial institutions, and telecommunications firms discussed emerging cyber threats and countermeasures.
- **Academic Institutions:** Cybersecurity researchers and university representatives provided analysis on trends in digital security education and capacity-building initiatives.
- **Civil Society Organisations:** Representatives from non-profits and advocacy groups explored ways to enhance public awareness of cybersecurity risks.

8. The State of Cybersecurity in South Africa by the CSIR

At the Cybersecurity Indaba 2024, **Mr. Samuel Lefophane**, a senior researcher at the **Council for Scientific and Industrial Research (CSIR),** presented key findings from their recent report on the state of cybersecurity in South Africa, published on 8 October 2024. The study, conducted in collaboration with the Cybersecurity Hub under the Department of Communication and Digital Technologies, offers a comprehensive overview of the nation's cybersecurity landscape.

Prevalence of Cyber Incidents

The survey revealed that 47% of organizations experienced between one to five cybersecurity incidents in the past year, highlighting the persistent threat environment. Alarmingly, 88% of participants admitted to suffering at least one security breach, with 90% of those organizations being targeted multiple times. Malware and phishing attacks emerged as the most common threats, underscoring the need for robust defense mechanisms.

Cybersecurity Awareness and Skills Gap

A significant concern identified was the lack of cybersecurity awareness among employees. Only 32% of respondents indicated that over half of their employees had received cybersecurity awareness training in the past year, pointing to a critical gap in building a security-conscious culture within organizations. Additionally, the study highlighted a substantial skills gap, with 63% of cybersecurity roles either partially or fully unfilled. Talent retention also poses a challenge, as 35% of professionals cited better offers, lack of training opportunities, and other factors as reasons for leaving their current positions.

Monitoring and Preparedness

The report found that only 41% of organizations assess and monitor cyber threats on a daily basis, indicating that the majority are not adequately prepared to deal with the high volume of cyber threats South Africa faces monthly. This lack of continuous monitoring leaves many organizations vulnerable to potential attacks.

8. The State of Cybersecurity in South Africa by the CSIR

Recommendations

To enhance the nation's cybersecurity posture, the CSIR recommends:

- **Enhanced Training and Awareness:** Implementing comprehensive cybersecurity awareness programs to educate employees about potential threats and best practices.
- **Addressing the Skills Gap:** Developing initiatives to attract and retain cybersecurity talent, including offering competitive incentives and continuous professional development opportunities.
- **Improved Monitoring:** Encouraging organizations to adopt regular and proactive threat monitoring practices to swiftly identify and mitigate potential risks.

By addressing these areas, South Africa can significantly improve its cybersecurity resilience, safeguarding its infrastructure and citizens from evolving cyber threats.

CSIR
Touching lives through innovation

9. Keynote Address by CEO of .ZADNA

In his keynote address, **Molehe Wesi**, CEO of .ZADNA, emphasised the role of cybersecurity in South Africa's digital transformation, particularly the government's responsibility in ensuring a secure digital ecosystem. He stated, *"If we have a safe internet ecosystem through the interventions of cybersecurity, I'm glad to say that people will buy more domain names."*

Wesi underscored the importance of **awareness, training, and skills development**, calling for a more inclusive approach that incorporates African teaching and learning systems. *"If you teach one, one will teach another—this is the approach we need when doing awareness campaigns."*

Highlighting the role of government in cyber resilience, Wesi stressed, *"Government needs to work with industry partners to ensure that digital hubs and innovation centres are used effectively, rather than becoming underutilised investments."* He pointed out that many government-led initiatives, such as digital innovation hubs, remain dormant due to a lack of partnerships within the ecosystem.

On cybersecurity as a national security imperative, Wesi warned, *"While South Africa has a cyber policy, it still remains to be tested. Our position in the global cybersecurity index shows that we are still behind, and this must be addressed urgently."*

He also highlighted the **risk posed to SMMEs**, stating, *"More than 60% of economic output relies on SMMEs. If they become a target, the economy collapses."* He urged the private sector and government to create **business continuity and disaster recovery strategies**, learning from incidents like the Transnet cyberattack that led to widespread economic disruptions.

In closing, Wesi made a call to action: *"This is not just a movement; it is a revolution. Cybersecurity must continuously evolve, and we need every stakeholder to engage, participate, and ensure that those most vulnerable are safeguarded."*

This keynote provided a strong foundation for the Indaba's discussions, reinforcing the need for strategic collaboration between government, industry, and academia in securing South Africa's digital future.

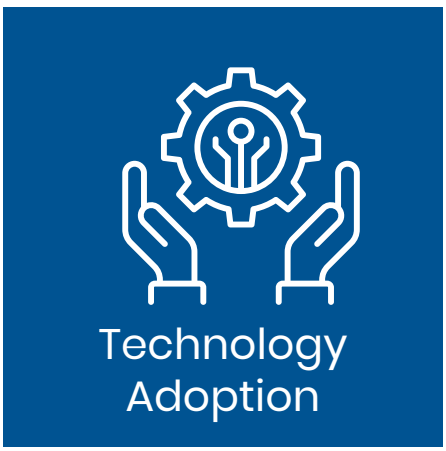
10. Survey Findings, Insights, and Recommendations

To gain deeper insights from participants, a comprehensive survey was conducted both during and after the Indaba. The survey aimed to capture attendees' perspectives on key cybersecurity issues, emerging threats, and areas for improvement. The 184 Participants provided valuable feedback on their experiences at the Indaba, the relevance of discussions, and their views on South Africa's cybersecurity priorities.

The post-event survey further allowed us to measure the impact of the Indaba and identify actionable recommendations for future engagements.

Recommendations Based on Survey Findings

Based on the insights gathered from survey responses, the following key recommendations are proposed:



10. Survey Findings, Insights, and Recommendations

1. **Regulatory Improvements**
   - Strengthen enforcement of **data privacy laws** and regulatory compliance.
   - Implement **mandatory cybersecurity policies** across high-risk industries.
   - Increase **government funding** for national cybersecurity initiatives.
2. **Technological Adoption**
   - Promote the use of **AI and automation** to enhance threat detection and response.
   - Improve security measures for **IoT devices** to prevent cyber vulnerabilities.
   - Encourage adoption of **blockchain and encryption** for securing sensitive data.
3. **Public-Private Collaboration**
   - Establish **information-sharing platforms** for cybersecurity intelligence.
   - Develop **joint cybersecurity task forces** between government and private sector.
   - Foster stronger engagement between **corporates, SMEs, and cybersecurity agencies**.
4. **Skills Development and Awareness**
   - Integrate **cybersecurity education** into school and university curriculums.
   - Expand **training programmes and professional certifications** for cybersecurity professionals.
   - Increase **public awareness campaigns** on online safety and cyber hygiene.

11. Conclusion and Way Forward

The **Inaugural Annual Cybersecurity Indaba 2024** successfully brought together key stakeholders to address South Africa's most pressing cybersecurity challenges. The event provided a much-needed platform for government representatives, industry leaders, academics, and civil society to collaboratively explore solutions, share insights, and commit to fostering a safer digital landscape. The discussions highlighted the urgent need for strategic investments in cybersecurity education, improved regulatory enforcement, and enhanced collaboration between public and private sector players.

A key takeaway from this Indaba is the need for a **sustained, coordinated effort** to drive cybersecurity awareness and resilience. The high turnout of academics and students demonstrates a growing interest in cybersecurity careers, which aligns with the national imperative to bridge the cybersecurity skills gap. Moving forward, educational institutions must work closely with industry stakeholders to equip students with practical skills and exposure to real-world cybersecurity challenges.

Furthermore, public-private partnerships must be strengthened to ensure effective threat intelligence sharing and collaborative cyber defense strategies. Cybersecurity cannot be the sole responsibility of government or industry leaders; it requires an ecosystem-wide approach. The private sector, particularly SMMEs and corporate enterprises, must actively invest in cybersecurity training, infrastructure, and response mechanisms to mitigate emerging threats.

12. Acknowledgements

We extend our sincere gratitude to the exceptional speakers who shared their expertise and insights, helping to drive forward crucial conversations around cybersecurity. A heartfelt thank you to **Molehe Wesi, Samuel Lefophane, Thulani Mabuza, Wayne Poggenpoel, Steve Jump, Neil Dundas, Sipho Mtombeni, Prof. Sizwe Lindelo Snail ka Mtuze, Tiyani Nghonyama, Prof. Elmarie Kritzinger, and Charmaine Strydom**. Your thought leadership has significantly contributed to shaping a more secure digital landscape for South Africa and beyond.

A special mention to **Matsetsebale Tleane from Agape Youth Movement** for expertly facilitating the programme, ensuring that the event ran seamlessly and that critical discussions were effectively guided.

We are immensely grateful to our partners whose support and collaboration were pivotal in making this Indaba a success. Your contributions helped create a platform that not only addressed urgent cybersecurity challenges but also showcased innovative solutions and strategies.

This event would not have been possible without the collective efforts and dedication of everyone involved. We deeply appreciate the opportunity to facilitate this important dialogue and look forward to furthering these discussions in future initiatives.

A special thank you to the incredible **CyberM8 Initiative team**: **Thabang Phala, Manqoba Mngomezulu, Doreen Mokoena, Sphokazi Ngobese, Otumiseng Motseothata, Bernice Binang, Prudence Mugwena**, and the amazing volunteers who played an instrumental role in making this event a success. Your hard work, dedication, and commitment are truly appreciated.

Together, we continue to build a safer and more resilient cybersecurity ecosystem. We look forward to the next Cybersecurity Indaba and furthering our collective mission to safeguard South Africa's digital future.

13. Next Steps: Cybersecurity Indaba 2025

Building on the success of the inaugural Indaba, we recommend hosting the **Second Annual Cybersecurity Indaba** in **October 2025**, aligning with **Global Cybersecurity Awareness Month**. This strategic timing will allow for greater international collaboration, knowledge-sharing, and alignment with global best practices in cybersecurity.

The **Cybersecurity Indaba 2025** will focus on:

- Expanding participation from key industries and government entities that were underrepresented in 2024.
- Showcase of the cybersecurity programmes implemented by CyberM8 and partners in 2024 and 2025.
- Presentation of abstracts by academics from various institutions of higher learning.
- Strengthening partnerships with **international cybersecurity organisations** to leverage global expertise and resources.
- Introducing more **interactive and hands-on cybersecurity simulations** to provide attendees with practical insights into cyber risk management.
- Driving policy recommendations that influence national cybersecurity regulations and enforcement mechanisms.
- Establishing a **year-round working group** to track progress on key resolutions from the Indaba and ensure continued engagement among stakeholders.

We call on both **public and private sector leaders** to be part of this initiative, not only in sponsoring and supporting the event but also in driving the execution of cybersecurity awareness campaigns and workforce development initiatives. The success of cybersecurity efforts in South Africa depends on **collective action**, and we urge all stakeholders to take an active role in shaping the country's cybersecurity future.

Together, we can build a stronger, more resilient digital ecosystem for South Africa. We look forward to reconvening at the **Cybersecurity Indaba 2025** and continuing our journey towards a safer digital future.

CYBERSECURITY INDABA | cyberm8

www.cybersecurityindaba.co.za

Contact Person
Manqoba Mngomezulu
manqoba@cyberm8.org.za
+27 83 368 6338