CYBERSECURITY INDABA 2025

Conference Report

Next-Gen Cybersecurity:
Innovating for Tomorrow's Challenges

Published March 2026

Prepared by

cyberm

Table of Contents

1. Foreword by the Conference Convener

Thabang Phala
CEO: CyberM8 Initiative NPC

The **Second Annual Cybersecurity Indaba** marks another important milestone in South Africa's journey towards building a secure, inclusive, and resilient digital economy. As our country accelerates its digital transformation agenda, cybersecurity is no longer a technical concern alone, it is a national priority that cuts across government, business, and society at large.

This year's theme, ***"Next-Gen Cybersecurity: Innovating for Tomorrow's Challenges,"*** reflects both the urgency and the opportunity before us. We are living in an era where emerging technologies such as artificial intelligence, cloud computing, and digital financial systems are reshaping how we live and work. At the same time, these advancements introduce increasingly sophisticated cyber threats that demand coordinated, forward-thinking responses.

A key message reinforced during this year's engagements is that cybersecurity is a shared responsibility. Government alone cannot address the complexity of cyber risks. It requires strong partnerships with the private sector, academia, and civil society to build the necessary skills, frameworks, and institutional capacity. Initiatives such as the Cybersecurity Indaba play an important role in advancing this multi-stakeholder approach.

Equally important is the focus on skills development and capacity building. South Africa must invest in developing a pipeline of cybersecurity professionals who are equipped to respond to evolving threats. By empowering young people, supporting research, and fostering innovation, we are laying the foundation for a more secure and competitive digital future.

We also recognise the importance of aligning our national efforts with continental and global frameworks. Cyber threats do not respect borders, and as such, collaboration across Africa and beyond is essential. The Indaba contributes to this broader vision by positioning South Africa as a leader in cybersecurity dialogue and innovation on the continent.

We extend our sincere appreciation to all partners, speakers, and participants who contributed to making the Second Annual Cybersecurity Indaba a success. Together, we are shaping a safer digital future for South Africa and the African continent.

2. Executive Summary

The **Second Annual Cybersecurity Indaba**, held on **29 October 2025** at **The Innovation Hub, Pretoria**, brought together key stakeholders from government, industry, academia, and civil society to engage on the future of cybersecurity in South Africa and across the African continent. Convened under the theme *"Next-Gen Cybersecurity: Innovating for Tomorrow's Challenges,"* the Indaba served as a national platform for dialogue, knowledge exchange, and partnership building in response to the rapidly evolving digital landscape.

The event featured high-level keynote addresses, panel discussions, research presentations, and skills-focused engagements that addressed critical areas such as financial cybercrime, artificial intelligence in cybersecurity, threat intelligence, policy and regulation, and cybersecurity skills development. The participation of local and international delegates further enriched the discussions, positioning the Indaba as a growing platform of continental relevance.

A key outcome from the Indaba was a strong call for **greater inclusivity in the cybersecurity ecosystem**. In his address, Mondli Gungubele emphasised the importance of ensuring that cybersecurity initiatives are inclusive and representative of all South Africans. This includes broadening participation across all demographic groups and creating equitable opportunities for skills development, innovation, and economic participation within the sector.

In addition, international delegates and stakeholders proposed the evolution of the platform into an **"Africa Cybersecurity Indaba,"** reflecting the need to expand the scope beyond South Africa and foster cross-border collaboration. This recommendation aligns with the growing recognition that cyber threats are transnational in nature and require coordinated responses across the continent.

Another significant outcome was the call to **strengthen private sector participation**, particularly by increasing the involvement of corporate organisations in shaping cybersecurity solutions, investing in skills development, and contributing to national and continental cyber resilience. This includes expanding partnerships with industry leaders, financial institutions, and technology companies to support innovation and implementation.

Collectively, these outcomes signal a clear strategic direction for the future of the Indaba: to become a more inclusive, collaborative, and continentally relevant platform that bridges policy, practice, and innovation.

The success of the Indaba was made possible through the support and collaboration of strategic partners from government, academia, and industry. Their contributions underscore the importance of a multi-stakeholder approach in addressing cybersecurity challenges and advancing South Africa's digital transformation agenda.

As the Indaba continues to grow, these insights and resolutions will inform the planning of future editions, ensuring that the platform remains responsive to the needs of the ecosystem while contributing meaningfully to building a secure and resilient digital Africa.

3. Overview of the Cybersecurity Indaba 2025

Overview

The **Second Annual Cybersecurity Indaba 2025**, held on **29 October 2025** at **The Innovation Hub, Pretoria**, was convened as a national platform to advance dialogue, collaboration, and action on cybersecurity in South Africa and across the African continent.

Hosted under the theme *"Next-Gen Cybersecurity: Innovating for Tomorrow's Challenges,"* the Indaba brought together key stakeholders from government, academia, industry, and civil society to address the growing complexity of cyber threats and the need for coordinated, forward-looking solutions.

With a strong focus on **academia, research, and innovation in cybersecurity** , the Indaba positioned itself as a bridge between policy, technical practice, and skills development. The programme reflected a deliberate effort to integrate research-led insights with practical industry applications, ensuring that discussions translated into actionable outcomes.

The Indaba also served as a catalyst for strengthening South Africa's digital transformation agenda by fostering partnerships, promoting knowledge exchange, and building a pipeline of cybersecurity skills that can respond to both current and emerging threats.

Objectives of the Indaba

The key objectives of the Second Annual Cybersecurity Indaba were to:

- **Facilitate Multi-Stakeholder Collaboration**
  Bring together government, academia, industry, and civil society to co-create solutions for cybersecurity challenges.
- **Advance Cybersecurity Skills Development**
  Address the growing skills gap by promoting training, education, and capacity-building initiatives aligned with the Fourth Industrial Revolution.
- **Promote Research and Innovation**
  Provide a platform for academic research presentations and encourage the integration of research into real-world cybersecurity solutions.
- **Strengthen National Cyber Resilience**
  Support discussions on policy, regulation, and institutional frameworks that enhance South Africa's ability to prevent and respond to cyber threats.
- **Encourage Industry Participation and Investment**
  Engage the private sector in shaping cybersecurity solutions, supporting innovation, and investing in skills development.
- **Position South Africa within the Continental Cybersecurity Agenda**
  Lay the foundation for broader African collaboration in cybersecurity through partnerships and knowledge exchange.

3. Overview of the Cybersecurity Indaba 2025

Key Themes and Discussions of the Indaba

The Indaba programme was structured to address critical areas shaping the cybersecurity landscape, combining keynote addresses, panel discussions, research presentations, and skills-focused sessions.

1. State of Cybersecurity in South Africa

The Indaba opened with a reflection on the current cybersecurity landscape, highlighting:

- ➔ Increasing cyber threats targeting both public and private sectors
- ➔ The need for improved national coordination and response mechanisms
- ➔ The importance of strengthening institutional and technical capabilities

This set the tone for the day by grounding discussions in the realities facing South Africa.

2. Cybersecurity Education, Research, and Innovation

The keynote address by the Deputy Minister focused on:

- ➔ The role of **education and research** in shaping the future of cybersecurity
- ➔ The need to align academic programmes with industry demands
- ➔ Building a sustainable pipeline of cybersecurity professionals

This reinforced the Indaba's central focus on **academia and innovation**.

3. Unlocking the Digital Economy Through Skills Development

This theme was explored through both an address and a panel discussion, focusing on:

- ➔ Closing the cybersecurity skills gap
- ➔ Aligning SETAs, universities, and industry training programmes
- ➔ Creating pathways for youth participation in the digital economy

Stakeholders emphasised the urgency of equipping young people with relevant digital and cybersecurity skills to support economic growth.

4. Collaboration Between Academia, Government, and Industry

A dedicated panel, powered by IITPSA, focused on:

- ➔ Strengthening partnerships across sectors
- ➔ Bridging the gap between research and industry application
- ➔ Developing scalable models for cybersecurity skills development in Southern Africa

This discussion highlighted that no single sector can address cybersecurity challenges alone.

3. Overview of the Cybersecurity Indaba 2025

5. Combating Financial Cybercrime

One of the most critical discussions of the Indaba focused on:

- ➔ The rise of **financial cybercrime**, including fraud, phishing, and cryptocurrency-related threats
- ➔ The role of **AI and emerging technologies** in both enabling and combating cybercrime
- ➔ The importance of **threat intelligence sharing and sector readiness**

The panel, powered by Absa, brought together regulators, law enforcement, and industry experts to provide a holistic view of the financial cybersecurity landscape.

6. Research Presentations and Knowledge Sharing

The Indaba featured two sessions of academic presentations, where:

- ➔ Researchers shared abstracts and findings on emerging cybersecurity topics
- ➔ Academia contributed to policy and industry discussions
- ➔ Opportunities were created for publication and further research collaboration

This reinforced the Indaba's positioning as a platform for **thought leadership and scholarly contribution**.

7. Closing the Cybersecurity Skills Gap – NextGen Skills Bootcamps

The **NextGen Skills Bootcamps session**, featuring organisations such as NEMISA and Google Cloud Security, focused on:

- ➔ Practical interventions to address the cybersecurity skills shortage
- ➔ Training programmes for youth and professionals
- ➔ Preparing the workforce for future cybersecurity demands

This linked directly to CyberM8's broader mission of skills development and empowerment.

8. Future Outlook and Strategic Direction

The Indaba concluded with a **Way Forward session**, outlining:

- ➔ Expansion of the Indaba into a continental platform
- ➔ Strengthening of partnerships and programmes under CyberM8
- ➔ Scaling initiatives such as HackSecure and skills bootcamps

This session translated the day's discussions into a forward-looking roadmap.

4. Cybersecurity Indaba 2025 Partners

5. Event Programme Overview

The **Second Annual Cybersecurity Indaba**, held on **29 October 2025** at **The Innovation Hub, Pretoria**, delivered a full-day, high-impact programme designed to drive dialogue, knowledge exchange, and collaboration across South Africa's cybersecurity ecosystem.

The programme was carefully curated to reflect the Indaba's theme, *"Next-Gen Cybersecurity: Innovating for Tomorrow's Challenges,"* with a strong focus on **academia, research, innovation, and skills development** .

The day commenced with **arrival and registration**, followed by a formal **welcome and opening remarks** by CyberM8 leadership, setting the tone for a purpose-driven engagement. This was immediately followed by a **State of Cybersecurity in South Africa** address, providing a grounded overview of the current threat landscape and national readiness.

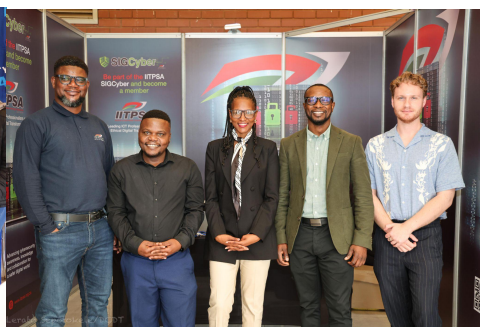
A high-level **keynote address** by the Deputy Minister of Communications and Digital Technologies highlighted the importance of cybersecurity education, research, and innovation in shaping South Africa's digital future. This was complemented by a strategic address from MICT SETA, focusing on unlocking the digital economy through skills development, as well as a partner address from Absa on the financial sector's role in securing Africa's digital ecosystem.

The programme then transitioned into a **multi-stakeholder panel discussion on cybersecurity skills development**, bringing together representatives from government, academia, and industry to explore collaborative approaches to closing the cybersecurity skills gap.

Mid-morning sessions featured **academic research presentations**, providing a platform for scholars and researchers to share insights and contribute to policy and practice. This was followed by a dedicated **panel discussion on strengthening collaboration between academia, government, and industry**, powered by IITPSA, reinforcing the importance of integrated approaches to skills development and innovation.

Following lunch and networking, the programme resumed with a presentation on the **State of Financial Crimes**, setting the stage for a high-level **panel discussion on combating financial cybercrime**. This session addressed emerging threats related to artificial intelligence, cryptocurrencies, and financial systems, while emphasising sector readiness and the importance of threat intelligence collaboration.

The afternoon continued with a second session of **academic presentations**, further deepening the research dimension of the Indaba. This was complemented by the **NextGen Skills Bootcamps session**, featuring partners such as NEMISA and Google Cloud Security, focusing on practical interventions to equip young people and professionals with future-ready cybersecurity skills.



6. Attendees Profile

The **Second Annual Cybersecurity Indaba** attracted a diverse and multi-sectoral audience, reflecting the growing importance of cybersecurity across all spheres of society. The event successfully brought together stakeholders from government, academia, industry, and civil society, creating a balanced and representative platform for engagement and collaboration.

Overall Attendance

The Indaba hosted an estimated **220 – 250 delegates**, including in-person participants from across South Africa, as well as a number of invited stakeholders and partners. The audience included senior decision-makers, technical experts, researchers, and emerging professionals in the cybersecurity ecosystem.

Sector Representation

The event achieved strong cross-sector participation, including:

- **Government and Public Sector**
  Representatives from national departments and public entities, including the Department of Communications and Digital Technologies (DCDT), Department of Science, Technology and Innovation (DSTI), and regulatory and law enforcement bodies.
- **Private Sector and Industry**
  Participation from financial institutions, telecommunications companies, cybersecurity firms, and technology providers, including organisations such as ABSA, MTN, Google, and other industry stakeholders.
- **Academia and Research Institutions**
  Academics, researchers, and students from institutions such as UNISA, Tshwane University of Technology (TUT), Wits University, and Nelson Mandela University contributed to both discussions and research presentations.
- **Professional Bodies and Industry Associations**
  Organisations such as IITPSA and other professional bodies contributed to knowledge sharing, accreditation, and skills development discussions.
- **Civil Society and Non-Profit Organisations**
  Representatives from NGOs and community-based organisations working in digital literacy, youth development, and online safety.




7. Contributors and Speakers

The **Second Annual Cybersecurity Indaba 2025** brought together a diverse group of speakers, facilitators, and knowledge partners from **government, academia, industry, and law enforcement**.

Key contributions came from institutions such as the Department of Communications and Digital Technologies (DCDT), Department of Science, Technology and Innovation (DSTI), MICT SETA, CSIR, UNISA, and leading private sector organisations including ABSA, Google, SABRIC, and MTN. Their participation ensured a balanced dialogue across policy, research, and practical implementation.

Through keynote addresses, panel discussions, and research presentations, speakers explored critical topics such as **cybersecurity skills development, financial cybercrime, and cross-sector collaboration**. Academic contributors added depth through research insights, while facilitators guided focused and meaningful discussions.

Collectively, their contributions strengthened the quality of engagement and reinforced the Indaba's role as a platform for collaboration, knowledge sharing, and innovation in cybersecurity.

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

Dr Namosha Veerasamy from the **Council for Scientific and Industrial Research (CSIR)** delivered a data-driven and insightful overview of the **State of Cybersecurity in South Africa**, drawing from the CSIR's 2024 research and industry analysis. Her presentation provided a comprehensive assessment of the current cybersecurity landscape, highlighting both systemic challenges and emerging risks.

A key insight from the presentation was that the **cybersecurity market in South Africa remains concentrated among a limited number of dominant players**, which presents both opportunities and constraints for broader industry participation and innovation. This market structure underscores the need to support the growth of small and emerging cybersecurity enterprises to diversify capabilities and strengthen the ecosystem.

Dr Veerasamy emphasised the **critical shortage of cybersecurity skills**, noting that the gap continues to hinder the country's ability to effectively respond to threats. This challenge is further compounded by a **lack of widespread awareness**, particularly among organisations and individuals who remain vulnerable to cyber incidents due to limited understanding of risks and preventative measures.

From a policy perspective, she highlighted that **South Africa's cybersecurity framework remains fragmented**, with multiple policies and initiatives that are not always fully aligned. This fragmentation limits the effectiveness of national coordination and response efforts, pointing to the need for a more integrated and cohesive policy environment.

The presentation also underscored the growing sophistication of cyber threats, particularly the increasing use of **artificial intelligence by threat actors** to automate attacks, enhance social engineering tactics, and evade traditional security controls. This evolution in the threat landscape calls for more advanced and adaptive cybersecurity strategies.

In response to these challenges, Dr Namosha stressed the importance of **stronger collaboration and cooperation across sectors**, including government, industry, and academia. She emphasised that combating cybercrime requires a collective approach, supported by shared intelligence, coordinated responses, and sustained investment in skills development and innovation.

Overall, her presentation provided a grounded and evidence-based perspective on the state of cybersecurity in South Africa, reinforcing the urgency of building a more inclusive, skilled, and collaborative cybersecurity ecosystem.

CSIR
Touching lives through innovation

9. Keynote Address Overview: Deputy Minister Mondli Gungubele

The keynote address by the Deputy Minister of Communications and Digital Technologies, Mondli Gungubele, set a strategic and forward-looking tone for the Second Annual Cybersecurity Indaba 2025. His address emphasised the central role of cybersecurity in enabling South Africa's digital transformation and safeguarding the country's growing digital economy.

He highlighted that as the nation continues to adopt emerging technologies such as artificial intelligence, cloud computing, and digital financial systems, the risk landscape is becoming increasingly complex. This calls for a coordinated national response that integrates **policy, innovation, and skills development**. He stressed the importance of strengthening institutional capacity, improving cyber resilience, and ensuring that cybersecurity is embedded across all sectors of the economy.

A key focus of his address was the urgent need to **develop cybersecurity skills at scale**, particularly among young people, to meet current and future demands. He underscored the role of education, research institutions, and training programmes in building a sustainable pipeline of skilled professionals.

The Deputy Minister also emphasised the importance of **inclusive participation in the digital economy**, calling for broader representation across all communities to ensure that no one is left behind in South Africa's digital future.

His address reinforced the need for **multi-stakeholder collaboration** between government, industry, and academia, positioning cybersecurity as a shared responsibility. Overall, the keynote provided a clear call to action for stakeholders to work collectively in building a secure, inclusive, and resilient digital ecosystem.






10. Address by MICT SETA on Skills Development in SA

In the keynote address, the MICT SETA Chief Executive Officer, Mr. Matome Madibana, highlighted the indispensable role of Sector Education and Training Authorities (SETAs) in enabling national digital transformation. The address, titled Unlocking South Africa's Digital Economy Through Digital Skills Development, underscored the importance of forward-looking investment in ICT human capital.

"South Africa stands at a defining moment. The global digital economy is projected to contribute over $20 trillion by 2030, but our success hinges on how fast we can equip our people with the right digital capabilities," said Mr. Madibana. "SETAs play a pivotal role in funding demand-driven programmes and building human capital that is agile, innovative, and ready for this future of work."

The CEO emphasised the cross-sectoral impact of these skills, noting that MICT SETA continues to drive collaboration across industries, academic institutions, and government to expand access to innovation hubs.

"Through strategic partnerships with institutions such as TUT, WITS Business School, and MLAB, we are investing in emerging technologies and innovation ecosystems that enable start-ups and SMMEs to thrive," Mr. Madibana added. "Our mission is not only to produce users of technology, but digital entrepreneurs who can build solutions for South Africa and beyond."

MICT SETA's initiatives are directly developing 4IR-aligned qualifications in Artificial Intelligence, Cybersecurity, Data Science, and Systems Development. More than 13,000 learners are supported annually through these digital skills programmes, with several locally developed digital solutions set for adoption by public sector institutions in 2026.

The Indaba was officially opened by the Deputy Minister of Communications and Digital Technologies, Mr. Mondli Gungubele (MP), who stressed the urgency of building a cyber-resilient South Africa.

"As our country digitises through initiatives like the National Digital and Future Skills Strategy, cybersecurity cannot be an afterthought, it must be the foundation of our digital transformation," said the Deputy Minister. "We must empower youth and women in the digital security field, invest in next-generation innovation, and embed cybersecurity into every national strategy."

As a transversal SETA, MICT SETA continues to lead national efforts to democratise access to digital technologies, foster cyber awareness, and strengthen South Africa's position in the global digital economy.

"Together, we can secure South Africa's digital future - one skill, one learner, and one innovation at a time," concluded Mr. Madibana.

11. The Financial Sector's Role in Securing Africa's Digital Future

Ms Maubate Kekana, Head of the Business Information Security Office (BISO) at **ABSA**, delivered a compelling and forward-looking address on the critical role of the financial sector in securing Africa's digital future. Her presentation emphasised that cybersecurity must extend beyond technical teams and become an **organisation-wide responsibility**, rooted in trust, awareness, and collective accountability.

She highlighted that in today's digital economy, financial institutions do not only safeguard money, but also **protect trust**, which is fundamental to customer relationships and economic stability. As she noted, *"Customers trust us with more than just their funds… it is trust that we actually sell to our customers."* This framing positioned cybersecurity as a business and societal imperative rather than a purely technical function.

Reflecting on Africa's rapid digital transformation, she underscored how technology has revolutionised financial services, enabling seamless transactions and expanding access to economic opportunities. However, this progress has also increased exposure to cyber risks. *"The more we bring technology to people, the closer the risk becomes,"* she cautioned, stressing the importance of bringing users along through awareness and education.

Ms Kekana further highlighted that key sectors such as **financial services, government, and telecommunications** remain primary targets for cybercriminals due to their central role in the digital economy. She illustrated the real-world impact of cyber incidents using global examples, demonstrating how attacks can disrupt operations, erode trust, and create widespread economic consequences.

A strong emphasis was placed on the **human element of cybersecurity**, noting that many cyber incidents originate from compromised credentials, social engineering, or lack of awareness. She reinforced that cybersecurity is not solely a technical issue, stating, *"Cybersecurity has become the connective tissue of trust that binds the digital economy together."*

11. The Financial Sector's Role in Securing Africa's Digital Future

Looking ahead, Ms Kekana addressed emerging risks and opportunities, particularly the role of **artificial intelligence and advanced technologies**. She noted that while threat actors are increasingly leveraging these tools, organisations must also adopt them to strengthen detection and response capabilities. In her words, *"The bad guys are good… which means we must be even better."*

She also outlined key priorities for securing Africa's digital future, including **security by design, cross-sector collaboration, talent development, and cybersecurity awareness**. She emphasised that collaboration and information sharing across industries are essential to effectively combat cyber threats, and that investment in skills development is critical to building long-term resilience.

Concluding her address, Ms Kekana delivered a powerful call to action, urging stakeholders to rethink their approach to cybersecurity:

- *"Beyond firewalls, we build trust."*
- *"Beyond compliance, we build confidence."*
- *"Beyond technology, we build a future."*

Her presentation reinforced the need for a **holistic, inclusive, and collaborative approach** to cybersecurity, positioning the financial sector as a key driver in safeguarding Africa's digital transformation journey.

Presentation Sponsored by ABSA

12. Academic Research Papers Presentation Overview

The academic track of the Second Annual Cybersecurity Indaba served as a critical forum for bridging the gap between scholarly research and industrial application. Chaired by **Prof Ephraim Sibanyoni** and **Dr Ayanda Ndlovu**, the sessions showcased diverse methodologies aimed at addressing South Africa's unique digital vulnerabilities. This report details the submission process, the thematic highlights of the presentations, and strategic recommendations for the national cyber ecosystem.

Session Proceedings

The presentations were strategically grouped and arranged according to their thematic alignment, focusing on Technical Innovation and Human-Centric Safety and Governance and Cyber Resilience

Chaired by: Prof Ephraim Sibanyoni and Dr Ayanda Ndlovu

Technical Innovation and Human-Centric Safety

Highlights: The session opened with a virtual presentation by **Ms Neo Onica Matsobane**, followed by an in-depth discussion on community-based safety frameworks by **Prof Wallace Chigona** and legal perspectives from **Adv Nandipha Ntsaluba**.

Governance and Cyber Resilience

Highlights: This session featured **Mrs Kudzayi Chegovo** and **Mr Ntwampe Mampuru**, focusing on organizational risk and the implementation of governance standards.

Key Themes and Research Highlights

The presentations provided a comprehensive look at the front lines of cyber defence:

- **AI and Machine Learning for Threat Detection:** The presentation by **Ms Neo Onica Matsobane** demonstrated a significant leap in malware detection. She detailed how Random Forest algorithms could achieve near-total accuracy in identifying malicious files, suggesting a shift away from static analysis toward dynamic, AI-driven defence.
- **Digital Safety in Education: Prof Wallace Chigona** delivered a compelling presentation on the "human layer" of security. He highlighted the urgent need for a **Cybersafety Community of Purpose** to protect learners in under-resourced schools, emphasizing that technical tools alone cannot solve social vulnerabilities.
- **Legal Frameworks and Digital Sovereignty:** The presentation by **Adv Nandipha Ntsaluba** addressed the complexities of the Cybercrimes Act. The discussion centered on the challenges of "borderless" crime and the necessity of harmonizing South African law with international standards to ensure effective prosecution.
- **Standardization of Information Governance: Mrs Kudzayi Chegovo** presented on the role of frameworks like ISACA in building organizational resilience. Her insights focused on creating robust audit trails to mitigate the financial and reputational damage of ransomware attacks.

12. Academic Research Papers Presentation Overview

Methodology and Impact

The presenters utilized a "socio-technical" approach, combining hard data with human-behavioural analysis:

- **Quantitative Modelling:** Using large-scale datasets to validate the efficiency of automated security tools.
- **Social-Ecological Research:** Analysing how schools and local communities interact with technology to identify points of failure in digital literacy.
- **Comparative Policy Analysis:** Reviewing existing South African legislation against global benchmarks to identify gaps in data privacy and criminal enforcement.
- **Impact:** These findings provide a roadmap for policymakers and industry leaders to move from "reactive" security to a "proactive" culture of resilience.

Recommendations and Way Forward

The 2025 presentations identified several pressing issues that require immediate response to strengthen South Africa's cyber ecosystem:

- **Establishment of Rural "Cyber-Hubs":** To address the vulnerabilities identified in schools, the country should invest in regional cybersafety agencies that empower local educators and community leaders to act as first-line defenders.
- **National AI Integration Strategy:** Given the efficacy of Machine Learning models presented, there is a clear need for a national standard for AI-driven threat detection in critical state infrastructure (water, electricity, and finance).
- **Public-Private Legal Synergy:** We must establish a faster pipeline between academic legal researchers and the National Prosecuting Authority (NPA) to refine how digital evidence is handled under the Cybercrimes Act.
- **The "Triple Helix" Approach:** The primary takeaway for the 2026 Indaba is the necessity of interdisciplinary collaboration. Future sessions should explicitly pair technical researchers (developers) with social scientists (behavioural experts) and legal scholars to ensure that new technologies are both safe and legally compliant.

Abstracts Presentations powered by UNISA: College of Law & CSIR

UNISA college of law

CSIR Touching lives through innovation

13. Survey Findings, Insights, and Recommendations

CyberM8 conducted a survey post the Indaba with a group of 50 participants from various sectors to gather their inputs and insights into the Indaba and its impact towards the Cybersecurity landscape in South Africa and the continent at large. The participants highlighted the following inputs:

- SA must focus on building its own data centres
- SA needs to empower the marginalised communities in the country in terms of skills developments
- Restructuring of the programme to incorporate all views from participants of the Indaba.

Recommendations Based on Survey Findings

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

13. Survey Findings, Insights, and Recommendations

1. **Research and Innovation**
   - Invest in next-generation cybersecurity research and innovation.
2. **Technology Adoption**
   - Increase of data centres in Africa.
   - Technology and data sovereignty.
3. **Public-Private Collaboration**
   - Strengthen public-private partnerships for digital resilience.
   - Inclusion of other African countries into the conversation.
   - Explore collaborations with other entities focusing on cybersecurity in Africa.
4. **Regulatory Improvements and Empowerment**
   - Modernise our laws to address emerging technologies like AI and quantum computing.
   - Embed cybersecurity into every national digital transformation strategy from health and education to infrastructure and industry.
   - Empower youth and women in the digital security field..

14. Conclusion and Way Forward

The **Second Annual Cybersecurity Indaba 2025** successfully brought together a diverse group of stakeholders to engage on some of the most pressing cybersecurity challenges facing South Africa and the broader African continent. Through a combination of keynote addresses, panel discussions, research presentations, and skills-focused sessions, the Indaba reinforced the importance of collaboration, innovation, and capacity building in strengthening cyber resilience.

A key takeaway from the Indaba is that cybersecurity is no longer a niche or technical issue, but a **strategic national and continental priority** that underpins economic growth, digital transformation, and public trust. The discussions highlighted critical challenges, including the cybersecurity skills gap, fragmented policy frameworks, the rise of AI-driven threats, and the need for stronger coordination across sectors.

Way Forward

Building on the outcomes of the Indaba, the following priorities will guide future engagements:

- ➔ **Expansion to a Continental Platform**
  Transition the event into the **Africa Cybersecurity Indaba** to strengthen cross-border collaboration and continental participation.
- ➔ **Inclusive Participation**
  Promote broader and more representative participation across all communities and sectors.
- ➔ **Private Sector Engagement**
  Increase corporate involvement in cybersecurity innovation, investment, and skills development.
- ➔ **Skills Development**
  Scale initiatives such as the **NextGen Skills Bootcamps** to address the cybersecurity skills gap.
- ➔ **Research and Collaboration**
  Strengthen partnerships between academia, government, and industry to drive innovation and knowledge sharing.

15. Acknowledgements

The **CyberM8 Initiative NPC** extends its sincere appreciation to all individuals and organisations who contributed to the success of the **Second Annual Cybersecurity Indaba 2025**.

We would like to express our deepest gratitude to our **strategic partners, sponsors, and collaborators**, whose support and commitment made this Indaba possible. We specifically acknowledge **ABSA** for its partnership and sponsorship, as well as the **Institute of Information Technology Professionals South Africa (IITPSA)** for its accreditation support and contribution to the academic programme.

We also extend our appreciation to our **government and public sector partners**, including the **Department of Communications and Digital Technologies (DCDT)**, the **Department of Science, Technology and Innovation (DSTI)**, and **MICT SETA**, for their leadership and contribution to shaping the national cybersecurity agenda.

Our sincere thanks go to our **academic and research partners**, including the **University of South Africa (UNISA) – College of Law**, the **Council for Scientific and Industrial Research (CSIR)**, **Tshwane University of Technology (TUT)**, **University of the Witwatersrand (Wits)**, and **Nelson Mandela University (NMU)**, for advancing research, innovation, and knowledge sharing within the cybersecurity ecosystem.

We further acknowledge the contributions of **industry partners**, including **MTN**, **Google Cloud Security**, **NEMISA**, **SABRIC**, **South African Reserve Bank (SARB)**, and other participating organisations, whose insights and expertise strengthened the quality of discussions and engagements.

Our appreciation also goes to all **speakers, facilitators, and panelists**, whose valuable contributions enriched the programme, as well as the **delegates and participants** who actively engaged in meaningful dialogue throughout the Indaba.

We would like to recognise the **CyberM8 team, organising committee, and volunteers** for their dedication and professionalism in delivering a successful event.

Finally, we thank all stakeholders and partners who continue to support our shared vision of building a **secure, inclusive, and resilient digital future** for South Africa and the African continent.

16. Next Steps: Africa Cybersecurity Indaba 2026

Building on the success of the inaugural Indaba, we recommend hosting the **Third Annual Africa Cybersecurity Indaba** in **October 2026**, 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 **Africa Cybersecurity Indaba 2026** will focus on:

- Continental cybersecurity strategies and frameworks.
- Strengthening partnerships with **international cybersecurity organisations** to leverage global expertise and resources.
- Driving policy recommendations that influence national cybersecurity regulations and enforcement mechanisms.
- TVET Colleges and skills development.
- Showcase of the cybersecurity programmes implemented by CyberM8 and partners in 2024 and 2025.
- Presentation of abstracts and research papers by academics from various institutions of higher learning.

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 **Africa Cybersecurity Indaba 2026** and continuing our journey towards a safer digital future.

Africa Cybersecurity Indaba

Africa Cybersecurity Indaba

www.cybersecurityindaba.africa

Follow Us on Social Media

LinkedIn: Africa Cybersecurity Indaba
Facebook, X, Instagram and TikTok: @CyberSecIndaba

info@cyberm8.org.za | +27 10 634 3619 | www.cyberm8.org.za