Cybersecure Conference

Cyber Secure
Guarding Tomorrow, Today

Building resilient digital futures: Navigating laws, threats, and innovation in South African Cybersecurity

29 & 30 September 2025

www.provisionresearch.co.za

Sandton Sun Hotel, Sandton, Johannesburg

Register now

EVENT OVERVIEW

In an era of escalating cyber threats and evolving regulations, South African organisations face unprecedented challenges in securing their digital landscapes. From sophisticated cybercrime impacting the economy to the complexities of new data protection laws and the imperative of integrating cutting-edge security architectures, the need for actionable insights and strategic foresight has never been more critical.

Cybersecure: Building Resilient Digital Futures is the indispensable event you cannot afford to miss. This comprehensive two-day seminar is meticulously designed to equip you with the knowledge and strategies to navigate South Africa's intricate cybersecurity environment with confidence.

Your presence at this conference is crucial as it offers unparalleled opportunities to master the national cybersecurity landscape, navigate South Africa's complex cyber regulatory framework, and ensure legal compliance. Financial institutions will gain essential insights into the Joint Standard for post-June 2025 compliance. Beyond technology, the event will empower you to build a human firewall, adopt modern security architectures such as Zero Trust and SASE, and responsibly leverage AI in cybersecurity. You will also learn to secure your supply chain, bridge the IT/OT divide for critical infrastructure protection, and build future-ready cyber defences against emerging threats.

Join us at the Sandton Sun Hotel to gain the cutting-edge insights, practical strategies, and networking opportunities necessary to future-proof your organisation against the evolving cyber threat landscape.

KEY BENEFITS:

- **N**avigate South Africa's intricate cyber regulatory framework, and ensure legal compliance with laws like POPIA (including 2025 amendments), the Cybercrimes Act, ECTA, and RICA.
- Financial institutions will gain essential insights into the FSCA's Joint Standard on Cybersecurity and cyber resilience for post-June 2025 compliance.
- Understand how to leverage AI-powered defence tools to enhance threat detection and automate responses, while also learning strategies to mitigate sophisticated AI-enabled attacks and develop responsible Generative AI governance policies.
- Shift to a proactive and adaptive security mindset, integrating cybersecurity into enterprise risk management to foster resilience as a fundamental business imperative.

Endorsed by:
Information Technology Association of South Africa.

ITA
The Information Technology Association of South Africa

"Cybercrime is the single biggest threat to every company on earth."
— Ginni Rometty, Former CEO, IBM

Day 1 - 29 September 2025

Building resilient digital futures: Navigating laws, threats, and innovation in South African Cybersecurity

08:00 - 08:45 Registration
08:45 - 09:00 Welcome

09:00 - 10:00 Session one: Keynote
Gain critical insights into the national cybersecurity landscape to enhance your defence

- Understand the cyber threats facing South Africa in 2025
- Review the economic impact of cybercrimes in South Africa
- Leverage government initiatives by aligning with South Africa's National Cybersecurity Strategy
- Engage in Public-Private Partnerships to collaboratively enhance the security of South Africa's digital infrastructure.

Prof. Noluntu Mpekoa, Deputy Director of the Centre for Cyber Security & Associate Professor, **University of Johannesburg's Academy of Computer Science and Software Engineering**

10:00 - 10:30 Coffee and networking

10:30 - 11:30 Session two
Master South Africa's cyber regulatory framework (POPIA, Cybercrimes Act & beyond) to ensure compliance and strengthen your cybersecurity

- Implement POPIA's core principles and understand its practical implications to ensure compliance and safeguard personal information across your business.
- Understand the Cybercrimes Act (19 of 2020), including criminalised cyber offences and general organisational obligations, to ensure compliance and avoid legal repercussions.
- Understand the roles of the Electronic Communications and Transactions Act (ECTA) and RICA to ensure compliance in digital security, data retention, and electronic transactions.
- Align with South Africa's National Cybersecurity Policy Framework to strengthen national cyber defence, incident response capabilities, and public-private cooperation.
- Understand regulatory convergence to develop a unified and effective compliance strategy that addresses interlinked laws.

Conrad Van Der Vyver, Director, **Van Niekerk Attorneys Inc.**

11:00 - 12:30 Session three
Roll out POPIA Amendments 2025 to secure your digital makeover and guarantee compliance

- Prepare for the POPIA Amendments 2025 by understanding their key updates, immediate effects, and operational impacts across industries.
- Streamline processes for enhanced data subject rights across all channels to ensure rapid, comprehensive compliance.
- Secure direct marketing by implementing strict "opt-in" consent, eliminating invalid "opt-out" for unsolicited communications.
- Clarify Information Officer responsibilities to continuously improve your compliance framework.
- Utilise practical guidance for the new eServices Portal to efficiently manage mandatory reporting of security compromises.
- Understand new administrative fine and instalment provisions to leverage enhanced payment flexibility.

Ashlin Perumall, Partner, **Baker & McKenzie**

12:30 - 13:30 Networking lunch

13:30 - 14:30 Session four: Panel discussion
Build a human firewall to cultivate strong security awareness and culture across your entire organisation

- Build effective security awareness programs that go beyond traditional failures to strengthen your human element and enhance overall security.
- How public institutions are building security awareness at scale
- Utilise effective training methodologies like gamification, interactive simulations, and continuous education to build a highly vigilant and security-aware workforce.
- Empower employees to identify and report suspicious activities without fear, fostering a robust reporting culture.

Confirmed speakers
-**Xolile Sibande,** Senior Manager for Information and Cyber Security (CISO), **Auditor-General of South Africa (AGSA)**
-**Dirk Labuschagne,** Chief Information Security Officer, **Direct Transact**
-**Thabiso Serake,** Head of Cybersecurity and TechOps, **Pay@**

14:30 - 15:30 Session five: Financial Institutions Focused
Discussion on the FSCA's Joint Standard on Cybersecurity and cyber resilience for financial institutions

- High-level overview of the Joint Standard 2 of 2024
- Why is the Joint Standard necessary?
- Examples of vulnerable financial institutions – is your pension safe?

Deirdre Phillips, Partner, **Bowmans Law**

15:30 - 16:00 Coffee and networking

Who should attend?

- **Cybersecurity Leaders & Practitioners:** CISOs, Security Managers, Security Architects, Analysts, and Engineers.
- **IT Professionals:** CIOs, IT Directors, Managers, Network Administrators, Cloud Engineers, and Infrastructure Specialists.
- **Legal & Compliance Officers:** Responsible for data privacy, regulatory compliance, and cybercrime-related legal risks.
- **Risk Management Professionals:** Focused on enterprise, operational, and cyber risk within business strategy.
- **Financial Services Professionals:** Focused on understanding and implementing the Joint Standard on Cybersecurity & Resilience.
- **Business Leaders & Executives**: Decision-makers driving cyber risk awareness, strategy alignment, and resilience.
- **OT & Infrastructure Stakeholders:** Securing control systems in energy, water, manufacturing, and transport.
- **HR & Training Specialists:** Focused on building security awareness and culture.
- **Procurement & Vendor Teams:** Manage third-party cyber risk and supply chain security.
- **Developers & DevOps:** Integrate security into the development pipeline.

From Public and Private sector

Day 2 - 30 September 2025

Building resilient digital futures: Navigating laws, threats, and innovation in South African Cybersecurity

09:00 - 09:30 Session six

Implement Zero Trust, SASE, and Cloud-Native Security to transform your architecture into a modern, highly secure defence

- Implement Zero Trust principles to fundamentally secure your hybrid work and cloud adoption with a "never trust, always verify" approach
- Carry out Secure Access Service Edge (SASE) to converge network security and WAN, effectively securing your distributed workforce.
- Adopt Cloud Security Posture Management (CSPM) to prevent misconfigurations across IaaS, PaaS, and SaaS cloud environments.
- Implement Cloud Workload Protection Platforms (CWPP) to secure workloads (VMs, containers, serverless functions) across your cloud environment.
- Deploy Cloud Identity & Access Management (CIEM) to effectively manage identities and entitlements, securing your cloud perimeter.
- Integrate DevSecOps in the cloud to embed security directly into your development pipeline.
- Addressing data residency, POPIA compliance for cloud data transfers, and local cloud adoption challenges.

09:30 - 10:00 Coffee and networking

10:00 - 11:00 Session seven

Harness the opportunities of AI in cybersecurity while mitigating its risks and ensuring responsible deployment

- Leverage AI-powered defence tools to enhance threat detection and automate detection and response to attacks.
- Implement strategies to mitigate sophisticated AI-enabled attacks like phishing, deepfakes, and adversarial AI techniques.
- Develop Generative AI governance policies to ensure safe, responsible employee use, prevent data leakage, and establish ethical AI practices.
- Address AI ethics and bias in security by implementing Responsible AI (RAI) and mitigating algorithmic biases.
- Understand South Africa's evolving stance on AI regulation and its impact on cybersecurity practices.

Corradino Corradi, General Manager - Information Security Strategy, Architecture and Technical Excellence, **MTN**

11:00 - 12:00 Session eight

Securing the supply chain by managing third-party cyber risk

- Understand the supply chain as a new attack vector to mitigate the exponential increase in supply chain attacks and their cascading impact.
- Identify and assess third-party risk through robust vendor due diligence, security ratings, and continuous monitoring.
- Embed strong cybersecurity requirements and accountability into vendor contracts through contractual security clauses.
- Manage software supply chain risks by addressing open-source components, software vulnerabilities, and secure development lifecycles (SDLC).
- Facilitate incident response with third parties through collaborative planning and communication for breaches involving vendors.

Emily Manganyi, Chief Information Security Officer, **JSE Limited**

12:00 - 13:00 Networking lunch

13:00 - 14:00 Session nine

Bridging the IT/OT divide for enhanced critical infrastructure protection

- Understand OT/ICS environments to secure operational technology in critical sectors like energy, water, manufacturing, and transport.
- Identify IT/OT convergence risks to mitigate new vulnerabilities from connecting isolated OT networks to IT systems.
- Mitigate threats to critical infrastructure by addressing escalating risks from state-sponsored attacks and hacktivism, causing physical disruption and service outages.
- Implement best practices for OT security, including network segmentation, asset inventory, patch management, physical security, and specialised threat detection.
- Secure the entire IoT Security Lifecycle, from design to decommissioning, by implementing device authentication, secure firmware updates, and data encryption.

14:00 - 15:00 Session ten

Build future-ready cyber defences against emerging threats

- Develop a Post-Quantum Cryptography (PQC) roadmap now to mitigate long-term quantum computing encryption threats.
- Implement strategies to attract, train, and retain skilled cybersecurity professionals.
- Understand the evolving cyber insurance landscape, including policy coverage and exclusions, to build a robust security posture essential for effective coverage.
- Shift to a proactive and adaptive security mindset, integrating cybersecurity into enterprise risk management, to foster resilience as a business imperative.

Godwin Dzvuke, Associate Director Cyber Security, **EGIT**

15:00 End of conference

What past delegates had to say?

"As an IT Specialist at ArcelorMittal South Africa, staying ahead of threats and compliance is paramount, and this event delivered practical strategies that were immediately applicable."— **IT Specialist, ArcelorMittal South Africa**

"The in-depth discussions on national cybersecurity strategy and public-private partnerships were exactly what we needed to enhance our resilience." — **GM ICT, City Power**

The conference is a must-attend for anyone in IT Security, Risk & Compliance. The deep dive into POPIA amendments and the Cybercrimes Act provided clarity on critical legal obligations." — **IT Security, Risk & Compliance, Pioneer Foods**