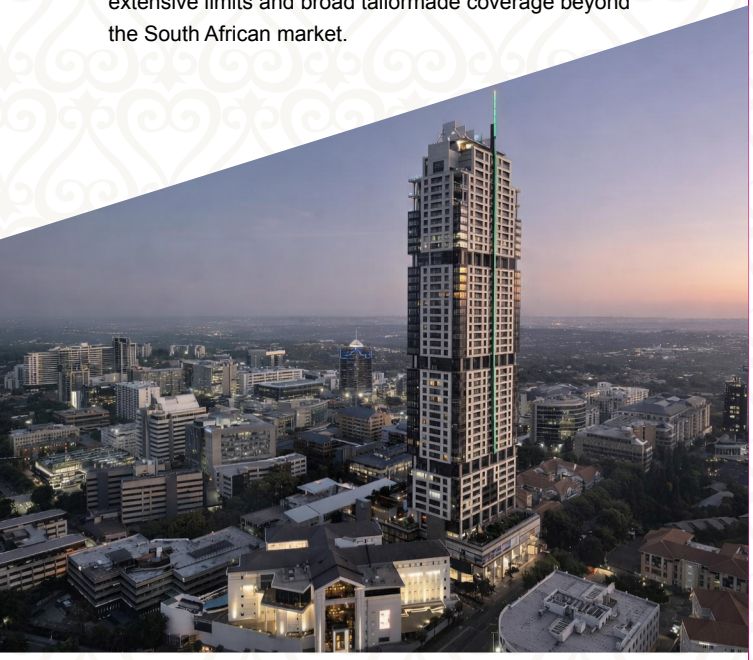
Why Sankofa for your Cyber insurances?

Focused Specialist Support for Your Risks

- **Public Sector Expertise:** Deep understanding of State-Owned Enterprises risks, governance and compliance.
- **Tailored Risk Solutions:** We can design cover that matches the unique governance and accountability risks of SOEs.
- **Governance Advisory:** Support for board training, compliance and aligning risk management with key principles.
- **Sankofa Team:** Decades of experience supporting a multitude of SOEs on Cyber risk solutions and providing the required support to clients on some of the largest Cyber incidents in South Africa.
- Access to an extensive Global Alliance network to source extensive limits and broad tailormade coverage beyond the South African market.



Disclaimer

- This brochure is a general overview and not meant to be generic. It does not replace professional advice or the terms of the policy wording.
- Sankofa's Professional Product Specialists (contact details below) are ideally positioned to discuss the variations in cover and arrange the required cover based on engagement.
- Risk Profiling considerations will be discussed including risk improvements in order to seek adequate coverage.
- Nuanced extensions and coverages can be explored to match individual requirements.

PREPARE FOR THE THREAT WITH PROTECTION FOR THE IMPACT.

Contact number: 011 025 6566
Email address: info@sankofaib.co.za
Website: www.sankofaib.co.za

SANKOFA
Insurance Brokers

An Authorized Financial Services Provider | FSP No. 44269

Major Cyber Attack Tonight:
Understanding the impact on your business tomorrow.

- **Exposure of sensitive data or disrupted services.**
- **Explanation to board, regulators and the public.** Steps you took to prevent it; seen as proactive and prepared, or reactive and negligent?
- Exact financial cost to your organisation for every hour systems are offline.
- Cyber threats currently inside your network that your security team has not detected yet.
- Which systems would cause the greatest operational or financial damage?
- Does your organisation have the financial protection and incident response capability to survive it?

Is this your most important Business Risk?

In today's digital economy, every organisation relies on technology, data, and connected systems.Unfortunately, this connectivity also exposes businesses to Cyber threats that can disrupt operations, damage reputations and create significant financial losses.

Sankofa Insurance Brokers can arrange the required protection, expertise and rapid response your organisation needs to recover from cyber incidents quickly and confidently.

From ransomware attacks to data breaches, our coverage solutions help protect your business from the financial and operational impact of Cyber crime.

What coverage can include:

Immediate response when it matters most

Cyber incidents require fast action. Our policy includes access to a network of cyber response experts.

24/7 Incident response team

Your organisation receives immediate support from specialists including:

- Cyber Security forensic investigators.
- Breach response experts.
- Data recovery specialists.
- Legal and regulatory advisors.
- Public relations and reputation management professionals.

These teams work quickly to contain the threat, minimise disruption and protect your reputation.

Data breach protection

Coverage for costs related to customer data breaches, including notification, legal support, and regulatory response.

Ransomware & Cyber extortion

Financial protection and expert negotiation support if your systems are targeted by ransomware attackers.

Business interruption

Compensation for lost revenue and operational downtime caused by cyber incidents.

Digital asset restoration

Coverage for restoring corrupted, stolen or destroyed digital data and systems.

Cyber Crime & fraud

Protection against losses resulting from phishing, social engineering, and electronic fund transfer fraud.

Media liability

Legal defence costs, legal liability to pay damages, public relations communication costs, and claims expenses arising from the performance of online media activities.

Notification expenses

Costs to notify affected parties and monitor any possible identity theft. Expenses incurred to comply with privacy legislation and includes legal and communication expenses.

Third party liability

Legal liability for damages to a third parties if you failed to prevent a Cyber incident on your computer system or other internet-connected components (network security).

Value Adds:
Proactive risk management tools

Modern insurance solutions go beyond simply reimbursing losses after an incident occurs. Many insurers now provide proactive risk management services designed to prevent or mitigate incidents before they happen.

These services may include:

Security and compliance guidance

Specialists assist organisations in strengthening controls and aligning with regulatory frameworks.

Incident preparedness

Organisations can gain access to crisis management plans, response protocols and simulation exercises.

Threat monitoring and intelligence

Services can include access to threat intelligence platforms and security alerts that help organisations detect emerging risks early.

Training and awareness

Insurance providers often support employee awareness programs to reduce risks associated with human error.

By integrating these services into the organisation's risk management strategy, insurance becomes a preventive and strategic tool, not merely a financial safeguard.