



Beyond Compliance: Leveraging the Cybersecurity Joint Standards for Business Value

Retirement Matters Seminar

Actuarial Society of South Africa

July 2025



The better the question. The better the answer. The better the world works.



Shape the future
with confidence

Agenda

1

- Industry trends

2

- Cybersecurity joint standard

3

- Practical implications & responses

4

- Questions

FSIs facing onslaught of cyber threats

74%

of large businesses experienced a significant or material breach in the last 12 months¹

#1

most targeted country in Africa for cybercrime as of 2025²

#1

most important global business risk for 2025³

100% increase

in Ransomware attacks
YoY with Q1 2025 already surpassing the total volume of attacks in 2024⁴

69%

of South African organisations reported being hit by a ransomware attack in 2024⁵

43%

of affected organisations paid the ransom with a median payment of R2,7m⁵

Absa reported a 400% increase in attempted cyber attacks over 2 years

Vishing accounts for 99% of Capitec's fraud cases

Online banking fraud accounts for 2nd highest losses according to SABRIC

¹ UK Government's Cyber Security Breaches Survey 2024

² ESET bi-annual threat report

³ Allianz Risk Barometer 2025

⁴ Osec Financial Services Threat Briefing June 2025

⁵ Sophos State of Ransomware in South Africa 2024

Recent high profile cyber attacks emphasise the need for more resilient ecosystems



Marks & Spencer

Third Party Breach
Sustained Online Disruption



Mediclinic

Third Party Provider
Personal Data Disclosure



Transunion

Data Access Breach
Regulatory Fines



NHLS

Ransomware
Widespread Outage

Prevalent types of cyber attacks



Malware

Damaging software such as viruses and ransomware

Users can be coerced to run the malware or an attacker can use other system vulnerabilities to enable them to run the malware



Phishing

Fraudulent attempts to steal information or gain access to systems through deceptive communications

E.g. fake emails, business email compromise, fake social media, phone calls, ad pop ups, etc.



Communication interception

Intercepting or altering communications between two parties or networks

E.g. Man-in-the-middle, session hijacking, eavesdropping



Authentication exploits

Compromising valid login credentials of users to gain unauthorised access to systems

E.g. Buying passwords from the darkweb, password guessing, SIM swapping to gain OTPs, exploiting reused passwords



Supply chain exploits

Targeting vulnerabilities in the supply chain to compromise security

E.g. compromising a supplier that has access to other networks, vulnerabilities in vendor software



Software flaws

Exploiting vulnerabilities and software errors

E.g. SQL injection, zero-day exploits, cross-site scripting



Denial of service

Overloading systems with traffic to prevent others from accessing the system, to disrupt the services or to cause the system to act in an unexpected way



AI-powered attacks

Using AI to enhance attacks by rapidly analysing systems for weaknesses, guessing passwords, predicting vulnerabilities or getting the AI systems to act in unexpected ways ('poisoning')

Boards and CROs rate cybersecurity as top risk

Top 10 CRO risk priorities for the next 12 months

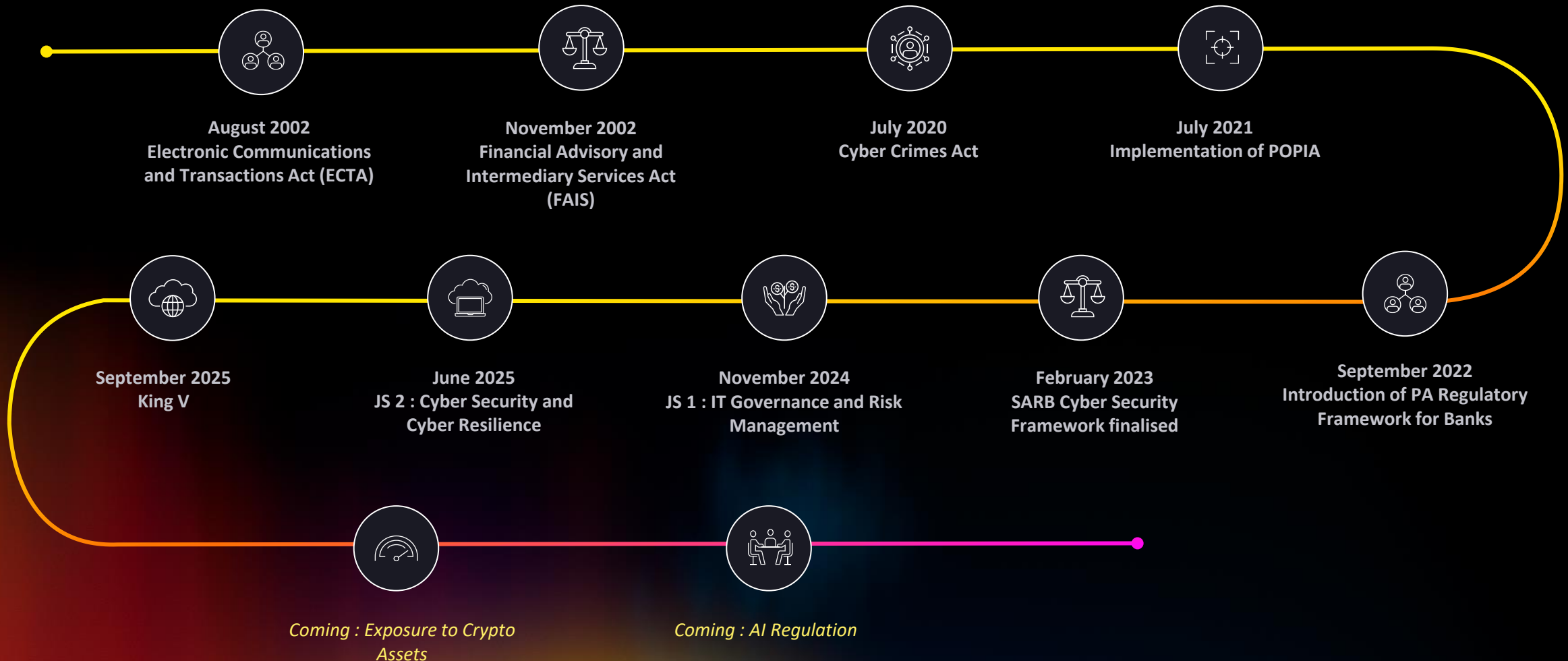


Top 10 Board risk priorities for the next 12 months

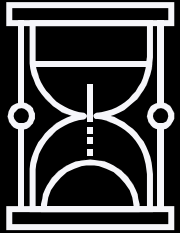


* In the CRO's view

Regulators introducing more pragmatic, enforceable, regulations



Joint standard 2 – Cybersecurity & Cyber Resilience



Commenced 1 June 2025

Hygiene

- Access management
- Privileged access management
- Multi factor authentication
- Network perimeter defence
- Vulnerability and patch management
- Secure configurations
- Malware protection

Fundamentals

- Identification
- Protection
- Detection
- Response and recovery
- Situational awareness
- Testing (including of 3rd parties)
- Learning and evolving

Crucial requirements

- 1 • Board level accountability
- 2 • Demonstrate compliance
- 3 • Independent assurance
- 4 • End-to-end ecosystem
- 5 • Risk based approach

Considerations for pension funds

Third-party (and 'nth' party) service providers like custodians and asset managers are desirable targets given the breadth of access they have to a variety of large clients. If compromised, all pension data held by these parties could be compromised. *What assurance is there that nth parties are effectively securing pension data and systems? How is pension data separated between different clients?*

Investment operations staff have access to sensitive pension information and the ability to make changes. They could be tricked or coerced into divulging information or redirecting investment funds. *Is staff adequately trained and aware of cyber attacks? Are there adequate SoDs to prevent inadvertent breaches?*

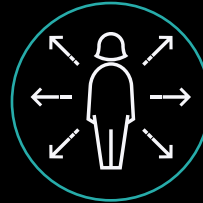
Pension providers' **websites** are by their nature readily available online. This exposes them to heightened risk of cyber attack. *How secure are the websites? What additional cyber protection is in place (e.g. multi factor authentication, encryption, firewalls)?*

Member and employer **portals** typically send, receive and store personal and sensitive information which is highly sought after by attackers for financial gain. Phishing scams are notorious for tricking users into divulging their credentials. *How sophisticated are authentication controls? How are users educated?*

Reports and **member data** is often stored in different places such as local drives or shared drives and communicated via email. *Is the data secured and accessible only to a limited number of authorised individuals who are aware of the risks and familiar with good controls? Are emails secured and encrypted?*



Spectrum of responses



Dedicated project with investment funding

Used as opportunity to transform cyber practices and mature capabilities

- Internal Audit fully engaged
- Board takes active interest
- Clear milestones and accountability
- Full ecosystem mapped and tiered
- Embedding requirements into existing policies, workflows, reports

Self-assessments and 'BAU'

Leveraging what is available internally to 'tweak' policies and processes to be able to demonstrate compliance

- Mapped existing policies and artefacts to requirements
- Seeking 'affirmation' rather than assurance
- Limited engagement with third parties

'Wait and see'

Uncertain about what to do and/or hoping for precedence to determine the 'minimum' required to comply

- Reluctant to involve 2nd or 3rd line
- Reliant on existing frameworks (e.g. NIST, ISO)

Challenges and roadblocks



Proportionality & materiality

Intuitively understand the benefit of a risk based approach but struggling to apply proportionality and materiality



Third party assurance

Both third parties and their use organisations are struggling to find a practical solution for demonstrating compliance / obtaining assurance



Board awareness

Although the requirement is for boards to take accountability, few organisations are taking a top-down approach



Sustainability of process

Embedding the requirements and evidence to demonstrate compliance into BAU processes, policies and reporting



Demonstrating compliance

Many organisations have conducted self assessments and readiness assessments. But organisations are struggling to distinguish between “demonstrating compliance” from “independent assurance”.



Uncertainty & precedence

Organisations are struggling to pre-empt how the PA/SARB will respond to the JS, especially as it relates to proportionality and demonstrating compliance

Practical solutions and industry responses

Industry forums

Sharing insights and experiences across the industry
Formulating guidelines to inform responses to the regulator.

Third party bureaus

Developing an industry-wide mechanism for obtaining third party assurance over ecosystem partners.

Mapping and tiering

Mapping data and system flows that can be used to visualise the critical areas.

‘Show your workings’

Utilising existing technologies and processes such as GRC tools to document decisions and risk assessments / tiering in support of proportional compliance.

Board awareness accountability

Using simulations to make the boards aware of their responsibilities; and take accountability for cyber strategy and oversight.



EY | Building a better working world

EY continues to deliver on its purpose – building a better working world – by creating new value for customers, people, society and the planet, and building trust in financial markets.

Through the use of data, artificial intelligence and advanced technologies, EY teams help clients to shape the future with confidence and to develop answers to the main challenges of today and of Omanis.

Operating in the fields of auditing, consulting, tax and legal assistance, strategy and transaction and backed by detailed industry analysis, a connected, multidisciplinary global network, and a diverse partner ecosystem, EY's professionals are able to provide a wide range of services in more than 150 countries and territories.

All in to shape the future with confidence.

EY means the global organisation of which the Member Firms of Ernst & Young Global Limited are members, each of which is an independent legal entity. Ernst & Young Global Limited, a Private Company Limited by Guarantee, does not provide services to clients. More information about EY's data collection and use and individual rights under data protection legislation can be found at ey.com/IT/privacy. EY Member Firms do not provide legal services where prohibited by local regulations. For more information about our organization visit ey.com.

© 2025 Ernst & Young Advisory Services (Pty) Ltd
All rights reserved.

ED None

This publication contains summary information and is therefore intended for guidance purposes only; it is not intended to be a substitute for a detailed study or a professional evaluation. EYGM Limited or the other member firms of the global EY organization assume no liability for losses caused to anyone as a result of acts or omissions taken on the basis of the information contained in this publication. For any specific matter, it is advisable to consult with a competent professional in the field.

ey.com