ICTS
LEGAL SERVICES

Cyber news that bites back
**Issue 5 • June 2026**

## SPECIAL UPDATE

# WHAT THE HACK?


NEWS

## CYBER SECURITY AND CYBER RESILIENCE INSIGHTS FROM ICTS LEGAL SERVICES

Dear Valued Clients and Colleagues,

**“Amateurs hack systems; professionals hack people.”**
- Bruce Schneier, renowned cryptographer and cybersecurity expert.

A HACK of a quote (think this through)

# AVBOB Cyber Incident: Lessons from a Trusted SA Institution Under Attack

In a stark reminder that no organisation is too established or essential to escape the growing wave of cyber threats, AVBOB Mutual Assurance Society - one of South Africa’s oldest and most respected funeral and assurance providers - confirmed a significant cyber incident this week. On or around 8 June 2026, the mutual society disclosed that external malicious actors had compromised its IT systems, leading to widespread disruptions in digital services.

AVBOB, which has served over 5.5 million South Africans for more than 100 years with funeral, burial, and insurance solutions, saw key online platforms go offline. Branches remained operational using manual processes for payments, claims, and arrangements, but the attack highlights vulnerabilities in third-party IT dependencies and digital transformation efforts common across the financial services sector.

**Key Details (as of 9-10 June 2026):**

- **Incident Discovery:** AVBOB became aware of the issue around 30 May. Investigations are ongoing to determine the full scope, including potential data exposure.
- **Impact:** Disruption to digital platforms and some branch services. Customers are advised they will not be penalised for payment delays.
- **Response:** Technical teams and specialist partners are working around the clock. AVBOB has notified the Information Regulator and is conducting a data audit.
- **Statement from Adriaan Bester, GM Corporate Affairs:** “The matter is being treated with the utmost seriousness… We prioritise continuity of essential services.”

This incident joins a troubling list of recent SA breaches affecting insurers (e.g. Liberty), government entities (Stats SA), and universities (Wits). South Africa ranks high in global breach statistics, with millions of accounts compromised over the years. For pension funds, retirement administrators, and asset managers, the message is clear: cyber resilience is not optional. Under Joint Standard 2 (and the upcoming COFI Bill requirements), organisations must demonstrate robust controls, incident response, and member communication.

**Practical Takeaways for Our Readers:**

1. **Review Third-Party Risks:** Many attacks exploit supply chain or outsourced IT. Audit your vendors rigorously.
2. **Incident Preparedness:** Test your Business Continuity/Disaster Recovery plans with cyber scenarios. Manual fallback processes saved AVBOB’s core services.
3. **Member Communication:** Transparent, timely updates build trust. AVBOB’s FAQ and branch assurances are good examples.
4. **Data Protection:** Assume breach and encrypt sensitive data. Monitor for phishing/social engineering that often precedes ransomware or destructive attacks.

AVBOB expects systems to recover in “days rather than weeks.”

# The Rise of AI-Powered Website Hacks: Indonesia as an Emerging Vector?

While the AVBOB attack represents a classic disruption incident, a parallel and evolving threat involves AI-enhanced cyber operations, with notable activity linked to actors in or emanating from Indonesia. Indonesia has long been a hotspot for hacktivism and cybercrime, but the integration of generative AI is supercharging capabilities - from automated phishing kits to sophisticated website compromises and reconnaissance.

Recent patterns show Indonesian-linked groups using tools that leverage AI for faster, more scalable attacks on websites and e-commerce platforms.

This includes:

- **Magecart-style skimmers** and carding operations that have hit hundreds of international sites.
- **Phishing kits and login portal cloning**, with past collaborations between US and Indonesian authorities highlighting the global reach (e.g. W3LL kit takedowns).
- Hacktivist defacements and DDoS, often targeting government or high-profile sites, now augmented by AI for reconnaissance, code generation, and evasion.
- Broader AI trends: Attackers use LLMs for custom malware, voice cloning in social engineering, self-replicating botnets, and automated vulnerability scanning of websites. Indonesia's rapid digital growth (AI adoption, fintech, e-commerce) outpaces cybersecurity maturity, creating fertile ground for both local threats and exported operations.

**Why This Matters for SA Financial Services:**

Pension funds, asset managers, and employee benefits platforms host sensitive member data on websites and portals. AI lowers the barrier for attackers - scripts that once took days to craft can now be generated in minutes, personalised at scale, or used to probe for weaknesses.

Indonesian actors have historically targeted regional sites; with cross-border data flows and global supply chains, SA organisations are not immune.

**Defensive Strategies:**

- AI for Good: Deploy AI-driven security tools for threat detection, anomaly scanning, and automated patching.
- Web Application Security: Implement WAFs, regular penetration testing, and zero-trust principles. Monitor for unusual traffic patterns.
- Awareness: Train staff on AI-amplified phishing (deepfakes, cloned sites).
- Regional Vigilance: Track indicators from highlighted regions – block access.
- Regulatory Alignment: Joint Standard 2 Phase requirements demand ongoing risk assessments - factor in AI threats explicitly.

The convergence of AI and cybercrime is accelerating. What was once the domain of sophisticated state actors is now accessible to mid-tier groups. Indonesia exemplifies how digital ambition without matching resilience creates exportable risks.

# Closing Note

*Cyber threats do not pause. The AVBOB incident and the global rise of AI-augmented attacks from regions like Indonesia underscore the need for proactive governance, investment in controls, and knowledge sharing.*

At ICTS Legal Services, we continue supporting pension funds, their providers, and trustees with compliance, assessments, risk management plans, training (ICTS Academy), and resilience strategies.

Questions or contributions? Contact us at ICTS Legal Services.

**What The Hack Newsletter**

Empowering Informed Defences.

Contact
Leon Greyling
082 464 5786
greylingl@icts.co.za


**What The Hack** is published monthly or when required. Past editions available on request.