ICTS
LEGAL SERVICES

Cyber news that bites back

Issue 2 • May 2026

NEWS

DEFINITIONS FROM JOINT

Standard 2 of 2024

CYBER INCIDENT UPDATES

South Africa in focus

THE HARSH REALITY

Snapshot (March - April 2026)

CYBERSECURITY AND CYBER RESILIENCE INSIGHTS FROM ICTS LEGAL SERVICES

Dear Valued Clients and Colleagues,

Welcome to the May 2026 edition of What The Hack, your monthly digest on global and local cybersecurity developments, brought to you by ICTS Legal Services. In an increasingly interconnected world, staying ahead of cyber threats is not just a technical necessity - it's a business imperative. This month we unpack the recent high-profile data breaches affecting major South African financial institutions, highlight notable global incidents, and provide a clear overview of the mandatory requirements under Joint Standard 2 of 2024 (JS2) for financial institutions.

We also include the official definitions of cybersecurity and cyber resilience straight from JS2, as these form the foundation of South Africa's new regulatory framework, plus the exact scope of who JS2 applies to.

Definitions from Joint Standard 2 of 2024

Cybersecurity means the preservation of confidentiality, integrity and availability of information and/or IT systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

Cyber resilience means the ability of a financial institution to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. It involves people, process and technology.

These definitions underpin JS2, which came into effect on 1 June 2025 and sets minimum standards for all financial institutions.

Scope of Joint Standard 2 of 2024
JS2 applies specifically to "financial institutions" as defined in the Standard itself. This is a tailored definition under the Financial Sector Regulation Act framework and covers the following entities (among others):

- **Banks**, branches of banks (including foreign branches), and their controlling companies (Banks Act, 1990);
- Mutual banks (Mutual Banks Act, 1993);
- **Insurers** and their controlling companies (Insurance Act, 2017);
- **Managers** of collective investment schemes (Collective Investment Schemes Control Act, 2002);
- Market infrastructures (e.g. exchanges, clearing houses, central securities depositories – Financial Markets Act, 2012);
- **Retirement funds** (pension funds) and administrators approved under section 13B of the Pension Funds Act, 1956;
- **Discretionary FSPs**, administrative FSPs, and certain Category I FSPs (including those providing investment fund administration services);
- OTC derivative providers; and
- Registered credit rating agencies.

The requirements are scalable: they must be implemented proportionately according to each institution's nature, size, complexity and risk profile, and the Standard must be read alongside other financial-sector laws.

Cyber Incident Updates: South Africa in Focus

South Africa continues to face sophisticated cyber threats targeting the financial sector. Two major incidents dominated headlines in March–April 2026:

- **Liberty Group SA (Liberty Life) Data Breach (March 2026):** Liberty detected unauthorised third-party access to select internal data systems. Client personal information - including names, ID numbers, and other details - was compromised. The company immediately contained the breach, confirmed that policies and investments remain secure, and notified affected clients via SMS and email. No impact was reported on core services or funds. Investigations are ongoing, with the Information Regulator involved.

- **Standard Bank Data Breach (March–April 2026):** Standard Bank identified unauthorised access to internal administrative and document-filing systems. Approximately 1.2 TB of client data (names, ID numbers, account numbers, contact details, and limited credit-card information) was exfiltrated by a threat actor known as "Rootboy." Core transactional banking systems were unaffected, and client funds remain secure. The bank has been notifying affected clients, monitoring credit bureaus and SIM-swap activity for fraud indicators, and cooperating with regulators. Data leaks have appeared online, heightening risks of phishing and identity fraud.

These linked incidents (Liberty is part of the Standard Bank Group) underscore the growing sophistication of attacks on financial data and the importance of rapid detection, containment, and client communication.

The Harsh Reality: What Hackers Do With Stolen Personal and Financial Data

When hackers steal data like that compromised in the recent Liberty Life and Standard Bank breaches, the consequences go far beyond the initial breach. Your personal and financial information becomes a valuable, tradable weapon on the dark web - and once it is out there, it can never be fully retrieved. Criminals treat it as currency, and the fallout can destroy lives and businesses for years.

Here's what actually happens to your stolen data:

1. **Immediate monetisation and resale:** Names, ID numbers, contact details, and account information are packaged and sold in bulk on underground forums - often within hours or days of the breach. Buyers include fraud rings, identity thieves, and even state-sponsored actors.

2. **Targeted identity theft and financial fraud:** Criminals use your exact details to impersonate you—opening loans or credit cards in your name, draining linked accounts, filing false tax returns, or committing insurance fraud. Your clean credit history becomes their golden ticket.

3. **Sophisticated phishing, vishing and account takeovers:** With real personal data in hand, attackers craft hyper-realistic scams (emails, calls, or SMS) that bypass your suspicion. SIM-swapping becomes child's play, allowing them to hijack your banking apps, email, and two-factor authentication.

4. **Long-term "dossier" attacks:** Your records are combined with data from other breaches to build complete identity profiles. What starts as one leak can haunt you for a decade - leading to repeated fraud attempts, blackmail using any sensitive details, or even reputational ruin if private information surfaces.

In these specific South African cases, portions of the stolen data (including names, ID numbers, and account details) are already being publicly released in batches on hacker forums. This dramatically escalates the immediate risk of fraud for every affected individual and company. Victims face drained bank accounts, ruined credit scores, years of constant monitoring, emotional trauma, legal battles, and massive recovery costs.

This is not hype - it is the documented playbook of modern cybercriminals. Your data is no longer private; it is now ammunition in someone else's hands. The seriousness must hit home: every day that passes without stronger defences is another day your clients, employees, and organisation remain exposed.

Global Cyber Incidents Snapshot (March - April 2026)

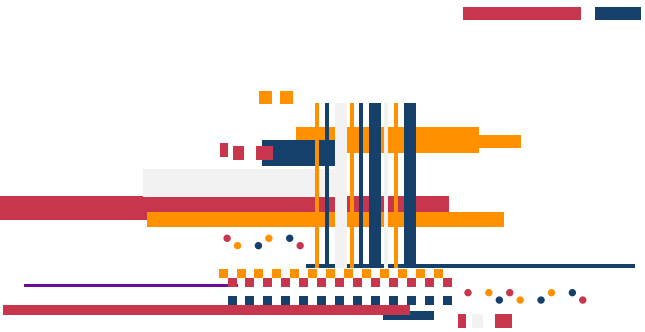
Cyber threats remain relentless worldwide:

Medical-device giant **Stryker** suffered a major cyberattack in March linked to an Iran-aligned group, disrupting operations, order processing, and shipping.

Multiple ransomware campaigns targeted healthcare providers, telcos, and tech vendors, with groups like Qilin and Crimson Collective claiming high-profile victims.

Large-scale credential exposures and API vulnerabilities continued to surface, affecting millions of records globally.

These events reinforce a clear trend: attackers are targeting critical infrastructure, supply chains, and personal data for financial gain and disruption



Regulatory Spotlight: What JS2 Requires of Financial Institutions

Joint Standard 2 of 2024 establishes mandatory, risk-proportionate requirements for cybersecurity and cyber resilience. All financial institutions must implement these measures according to their nature, size, complexity, and risk profile. Key obligations include:

- **Governance & Oversight** - The governing body (Board) is ultimately accountable for cyber risk. It must ensure a dedicated cybersecurity function with adequate resources, clear roles and responsibilities (including three lines of defence), and direct reporting lines. An independent oversight function may be required.
- **Cybersecurity Strategy & Framework** - Establish and maintain a Board-approved strategy aligned with business objectives. Review it at least annually to address evolving threats, close gaps, and incorporate lessons learned. Define measurable risk tolerances, metrics, and reporting.
- **Risk Management & Asset Identification** - Identify and classify all critical business processes, information assets, and third-party dependencies by criticality and sensitivity. Maintain an up-to-date asset inventory (reviewed at least every two years). Conduct regular risk assessments.
- **Protective Controls (Cybersecurity Hygiene & Defence-in-Depth)** - Implement robust identity and access management (including strong authentication and MFA for remote/admin access); data-loss prevention and encryption policies; secure application/system development; network segmentation, firewalls, and intrusion prevention; cryptography key management (where used); and mandatory annual cybersecurity awareness training for all staff and the Board.

- **Detection & Monitoring** - Deploy continuous monitoring capabilities (e.g., a Security Operations Centre or equivalent) to detect anomalies, collect and correlate logs, and enable timely response.
- **Incident Response & Recovery** - Maintain comprehensive incident-response policies, plans, and processes (including communication protocols). Ensure secure, tested backups with defined recovery-time and recovery-point objectives. Rapidly contain, eradicate, and recover from incidents while minimising systemic risk.
- **Testing & Assurance** - Conduct regular vulnerability assessments, penetration testing (including black-box where appropriate), scenario-based simulations, and independent reviews of the entire framework. Remediate findings promptly.
- **Third-Party & Outsourcing Risk** - Apply the same standards to outsourced services and third-party providers. Include cybersecurity requirements in contracts, conduct due diligence, and ensure ongoing oversight.
- **Reporting & Cooperation** - Promptly notify the Prudential Authority and Financial Sector Conduct Authority of material cyber incidents. Cooperate with sector-wide resilience efforts.

JS2 must be read alongside other financial-sector laws and is designed to be practical and scalable. Non-compliance carries regulatory and reputational consequences.

CLOSING THOUGHTS

The Liberty and Standard Bank incidents - coupled with the terrifying reality of what happens to stolen data - serve as timely reminders that even well-resourced institutions can face significant exposure. JS2 provides a clear roadmap for strengthening defences and building true resilience. ICTS Legal Services remains ready to assist with compliance assessments, policy reviews, incident-response planning, and regulatory engagement.

If you would like a gap analysis against JS2, assistance with breach notification obligations, or a tailored workshop for your team, please contact us.

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

What The Hack is published monthly. Past editions available on request.