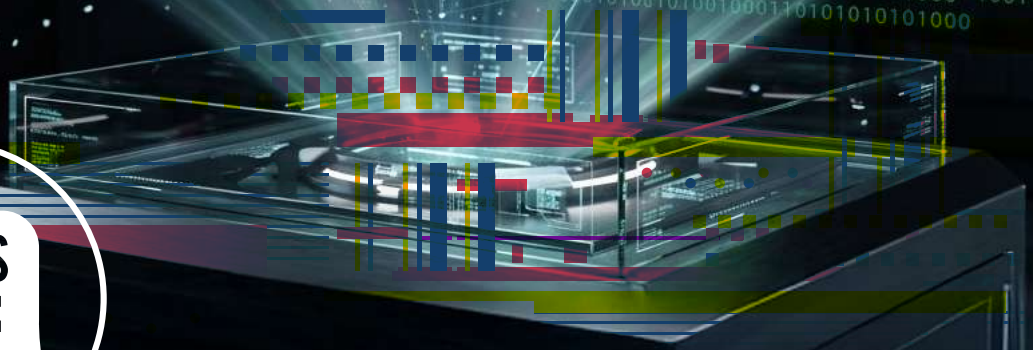
ICTS
LEGAL SERVICES

Cyber news that bites back

Issue 1 • April 2026

WHAT THE HACK?



NEWS

RECENT HACKING ACTIVITY

South Africa First and Global Roundup

COMMON FINDING

from Joint Standard 2 assessments

GOOD PRACTICES

to avoid the next hack

South Africa First

South Africa continues to face intense cyber pressure, with both government and financial services sectors firmly in the crosshairs. In March 2026 alone, cybercrime group **XP95** claimed responsibility for two devastating attacks on government entities. They breached the **Gauteng Provincial Government**, stealing 3.8 TB of personal data - including 3,673,556 files with IDs, CVs and job-seeker records - then listed the haul for sale on the dark web for just $25,000 (roughly R420,000). Days later, **Statistics South Africa (Stats SA)** confirmed its systems had been compromised by the same group. XP95 exfiltrated 453,362 files (154 GB) and demanded a R1.7 million ransom. The breach has triggered national security concerns because Stats SA holds census, economic and demographic data used by every government department and business in the country.

Adding to the strain on critical sectors, major financial services provider **Liberty Group SA** (owned by Standard Bank) disclosed a significant data breach on 24 March 2026. The company detected unauthorised third-party access to select data systems, exposing personal information - including names, surnames and ID numbers - of certain clients. Liberty promptly notified affected customers via SMS, launched a full investigation (complying with POPIA), and assured clients that policies, investments and core services remain secure and fully operational. No specific threat actor has been named and the full scope is still under review.

Earlier in January 2026, the **Land and Agricultural Development Bank of South Africa (Land Bank)** was paralysed by a ransomware attack from a ransomware-as-a-service group. Hackers exfiltrated and encrypted files before demanding R5.7 million in Bitcoin. The incident forced key services offline and underscored the vulnerability of state-linked financial institutions. The numbers paint an even darker picture. In January 2026 alone, South African organisations faced an average of 2,145 cyber attacks per week - a 36 % year-on-year surge. Across Africa, SA now ranks as the most attacked economy, with data breaches occurring every three hours and a staggering 60 % rise recorded in the first half of 2025. Experts warn that 90 % of these incidents were preventable with basic controls.

Global Roundup

Financial services and insurers remain prime targets worldwide. In Germany, major health insurer **HanseMerkur** was hit in early February 2026 by the DragonForce ransomware group, which claims to have exfiltrated nearly 97 GB of internal corporate data - including financial documents, invoices, tax records and files linked to its UAE partner Emirates Insurance. The company has not yet publicly confirmed the full impact.

In the US, **Allianz Life Insurance** disclosed a major supply-chain breach (July 2025, still rippling into 2026 notifications) that compromised personal data - including names, SSNs, addresses and more - of roughly 1.5 million customers, financial professionals and employees after attackers used social engineering to access a third-party cloud CRM system.

The rest of the world is hardly safer. February and March 2026 delivered several headline-grabbing incidents:

- Dutch telecom **Odido** disclosed a breach affecting 6.2 million customer records (names, phone numbers, emails, bank details and passport numbers).
- **ShinyHunters** struck again, hitting dating giant **Match Group** (Tinder, Hinge, OkCupid) with 10 million records exposed and online-auto marketplace **CarGurus** with 12.4 million user accounts.
- **Panera Bread** confirmed 5.1 million customer accounts leaked after a failed extortion attempt.
- Medical-tech firm **Stryker** suffered a mass device-wipe attack linked to an Iran-aligned hacktivist group.
- Ransomware slammed **University of Mississippi Medical Centre** (forcing clinic closures) and telecom provider **Brightspeed** (1 million+ users affected).

Anecdote worth noting: nation-state actors are no longer just spying - they're "pre-positioning" inside critical infrastructure for future activation. The time from network intrusion to data theft has collapsed to just 72 minutes globally (down from 285 minutes in 2024). South African organisations, sitting on vital logistics and ports, are squarely in the firing line.

Hackers who access stolen data typically aim to monetise it quickly and efficiently through several primary channels: selling large datasets of personal identifiable information (PII) such as names, ID numbers, emails, phone numbers, and financial details on the dark web to other cybercriminals, who then use them for identity theft, opening fraudulent accounts, applying for loans or credit cards in victims' names, or committing tax and benefits fraud.

In cases involving ransomware, attackers encrypt the data and demand payment (often in cryptocurrency) to restore access or threaten to leak or sell it publicly if unpaid, while in other breaches they leverage credentials for account takeovers, credential stuffing attacks across multiple platforms, or sophisticated phishing campaigns tailored with the stolen details to extract even more value. Beyond direct financial gain, nation-state actors or hacktivists may exfiltrate data for espionage, competitive intelligence, or public exposure to cause reputational damage, but the overwhelming majority of opportunistic cybercriminals treat the haul as a commodity - bundling and reselling it in bulk - to fuel further crimes like medical identity theft or extortion, turning one breach into cascading harm for individuals and organisations long after the initial intrusion.

COMMON FINDINGS FROM JOINT STANDARD 2 ASSESSMENTS

With close on 100 service providers assessed over the past 6 months, certain lessons have emerged:

1. **Cyber insurance**
   Don't automatically assume your providers hold cyber insurance, let alone sufficient cyber insurance.

2. **Failure to complete questionnaires**
   While most providers are responding to detailed questionnaires on the status of their cybersecurity and resilience measures, some are simply providing a letter of assurance. In some cases this may be sufficient for trustees to rely on, but in several cases, not.

3. **Range of scores**
   Sub-category assessment scores generally range between 2 and 4,5 out of 5 across providers. Overall, most providers rate as medium to medium-low risk.

4. **Abuse of proportionality**
   Some providers are relying on the principle of proportionality to opt out of building the required levels of cyber security and resilience. This places trustees at risk and should not be accepted. Also, proportionality does not allow funds to simply ignore the Standard.

GOOD HYGIENE PRACTICES TO AVOID THE NEXT HACK

Ninety percent of South African breaches are preventable. Here are the non-negotiables that actually move the needle:

1. **Turn on Multi-Factor Authentication (MFA) everywhere**
   It still blocks 99 % of automated account takeovers. Mandate it for email, banking, cloud admin consoles and third-party apps - no exceptions.
2. **Patch ruthlessly**
   The average breakout time for ransomware is now 29 minutes. Apply critical security updates within 48 hours of release. Use automated patch-management tools and test in staging first.
3. **Run mandatory phishing simulation training quarterly**
   Phishing remains the entry vector in 42 % of breaches. Make training short, realistic and measured by click-rate reduction - not just completion certificates.
4. **Adopt the 3-2-1 backup rule**
   Three copies, two different media types, one off-site and air-gapped. Test restores monthly. Ransomware operators love finding that one untested backup.
5. **Enforce strong, unique passwords + a password manager**
   The 149-million credential dump discovered in January 2026 proves reuse is still rampant. Ban password sharing and expired credentials.
6. **Implement basic Zero-Trust principles**
   Verify every user, device and application - every time. Least-privilege access and micro-segmentation stop lateral movement once the perimeter is breached.
7. **Monitor, monitor, monitor**
   Deploy endpoint detection and response (EDR) with 24/7 SOC coverage or managed detection services. The earlier you spot the anomaly, the cheaper the incident.

FACT: Global ransomware damage is forecast to hit USD 74 billion in 2026. In South Africa the average breach already costs organisations millions in downtime, regulatory fines and lost trust. Basic hygiene isn't optional - it's the cheapest insurance policy you'll ever buy.

Sources: UpGuard, ITWeb, MyBroadband, EWN, Cybernews, SecurityWeek, BleepingComputer, Check Point Research, Unit 42 Incident Response Report and public disclosures as of 31 March 2026.

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