ICTS
LEGAL SERVICES

Cyber news that bites back

Issue 4 • June 2026

Update

WHAT THE HACK?

NEWS

UNIVERSITY OF THE WITWATERSRAND (WITS)

Cyber Incidents

CYBER INCIDENTS IN SOUTH AFRICA'S

Financial Services Sector

CYBER ATTACK STATISTICS

Biggest Losses, Settlements, and Downtime

Dear Valued Clients and Colleagues,

*Welcome to another edition of **What The Hack**, your monthly roundup of the wild world of cybersecurity incidents, breaches, and the evolving threat landscape. As we head into the middle of 2026, ransomware gangs, supply-chain attacks, and data extortion continue to dominate headlines. Let's dive in.*

But first, a Hack of a Joke....

Why was the computer cold?

It left its Windows open.

Spotlight: University of the Witwatersrand (Wits) Cyber Incidents

South Africa's University of the Witwatersrand was hit by multiple incidents in recent months. In May 2026, Wits was caught up in a global data breach targeting Instructure's Canvas learning management system (Ulwazi at Wits). The threat actor group ***ShinyHunters*** claimed responsibility, stealing user data including names, email addresses, student numbers, and messages (but reportedly not passwords or financial info).

The group issued a ransom demand and set a deadline of May 12, 2026, threatening to leak the data if no settlement was reached. Wits and other affected institutions (including Stadio and SPARK Schools) urged vigilance against phishing. The university restored its learning platform after brief downtime following patching and testing.

Separately, Wits' Oracle E-Business system was impacted by a broader cyberattack in late 2025 that affected multiple countries. The university worked with experts and Oracle to assess the breach.

These incidents highlight the vulnerabilities in educational tech supply chains and the growing pressure from extortion groups.

Closer to Home: Recent Cyber Incidents in South Africa's Financial Services Sector

1. Alexforbes CEO Email Accessed in Business Email Compromise (BEC) Attack (late April 2026)

- Attackers compromised the CEO's legitimate work email and used it for a targeted Business Email Compromise (BEC) phishing campaign, sending fake "revised order" PDF attachments to clients/stakeholders.
- Response: Account immediately blocked; direct warnings issued; clients advised to delete emails, avoid attachments/links, change passwords, and scan devices. No wider system breach or client retirement-fund data exposure reported.
- Why it matters: Highlights risks to high-privilege executive accounts even in sophisticated organisations. Reinforces need for Multi Factor Authentication (MFA) on email, advanced BEC/phishing detection, and ongoing awareness training. Prime targets are retirement-fund data.

2. Liberty Group SA Data Breach (March 2026)

- Unauthorised third-party access to select internal data systems; personal customer information exposed. Policies, investments, and services remained secure/operational.
- Response: Immediate containment + investigation; affected clients notified via SMS/email; security review underway (possible enhanced controls).
- Why it matters: Another major SA financial player hit; personal data exposure raises identity theft/phishing risks and erodes trust. Transparent communication and access controls are critical for entities handling retirement savings.

3. Standard Bank Data Exfiltration (Rootboy Attack) (late Feb–March 2026)

- Threat actor "Rootboy" accessed internal administrative/document filing systems for appr. 3 weeks and exfiltrated c.1.2 TB of data (names, IDs, account numbers, contacts, limited credit card info). Data publicly dumped on dark web/forums. Core transactional banking systems and client funds not accessed.
- Response: Multiple client updates with protective guidance; working with Information Regulator and authorities; enhanced monitoring/fraud detection; customers advised to change passwords, enable extra security, monitor accounts, and watch for phishing.
- Why it matters: One of the largest recent SA banking data incidents. Shows attacker persistence, value of "non-core" internal data, and detection/segmentation gaps. Downstream risk for retirement fund members who bank there. Reinforces zero-trust, continuous monitoring, and sector threat-intelligence sharing.

- Enforce MFA + privileged access management + advanced email/BEC detection everywhere (especially executive accounts).
- Assume breach is possible - verify, don't trust (especially payment/document requests).
- Network segmentation, encryption, and continuous monitoring/anomaly detection are essential for member/admin systems.
- Have tested incident response + transparent client notification playbooks ready.
- Robust third-party/vendor cyber due diligence and contractual requirements (many incidents originate via interconnected systems).
- Sector collaboration on threat intelligence is increasingly valuable.

Summary: These incidents (plus the Ekurhuleni R2bn + heist) show no organisation is immune. Retirement funds and providers must take cybersecurity seriously.

Other Notable Hacks and Breaches (Recent Months)

- **Supply-Chain and Vendor Attacks:** Multiple U.S. banks (e.g. Citizens Financial and Frost Bank) were hit via a shared third-party vendor in April 2026. Everest ransomware was linked.
- **Healthcare and Tech:** Medtronic faced claims from ShinyHunters involving up to 9 million records. Stryker experienced a major cyberattack with device wipes and disruptions.
- **Credential Leaks:** Massive exposures continued, including a 149 million record database dump early in 2026 and ongoing credential-stuffing dumps affecting billions of records across platforms.
- **Ransomware Rampage:** Groups like Qilin, ShinyHunters, and newcomers (e.g. Crimson Collective) claimed victims including telecoms (Brightspeed - over 1mn users), retailers, and more. Nike reportedly investigated a 1.4 TB internal data theft.
- **Other High-Profile:** Attacks on airlines (e.g. WestJet disruptions), government systems (e.g. Vietnam ministerial networks), and education/research institutions persisted.

The trend? Attackers increasingly exploit trusted vendors, and third-party integrations rather than direct breaches - retirement funds to note!

Cyber Attack Statistics: Biggest Losses, Settlements, and Downtime

Cybercrime costs continue to soar, with global estimates projecting **$10.5 trillion+ annually**. Here are standout 2025–2026 stats:

- **Average Data Breach Cost:** Around $4.44–4.88 million globally (higher in the US at c.$10M+ for some sectors). Healthcare remains the most expensive (c.$10.9M average).
- **Ransomware Impact:** Annual damages forecasted near $74 billion in 2026. Average downtime costs businesses **c.$53,000 per hour**. Recovery often costs 10x the ransom demand.

Largest Incidents:

- Credential leaks: 16 billion+ passwords exposed in major dumps.
- Record breaches: Incidents affecting 100M+ records (e.g. Meta/Facebook claims in prior periods, massive Chinese leaks).
- Economic Damage: UK incidents like one costing £1.9B; supply-chain attacks disrupting operations for thousands of organisations (e.g. MOVEit legacy impacts still felt).
- **Frequency:** Thousands of attacks weekly; phishing and ransomware dominant. Education sector saw notable ransomware spikes.

Downtime from DDoS or ransomware can cost **$6K–$120K per minute** for affected businesses, underscoring the need for resilience.

And now for something completely different!

Ethical hacking, also known as white-hat hacking or penetration testing, is the authorised and legal practice of deliberately attempting to breach computer systems, networks, applications, or infrastructure to identify vulnerabilities before malicious actors can exploit them. Unlike criminal hacking, it is performed with explicit written permission from the system owner, within a clearly defined scope (known as Rules of Engagement), and with the goal of improving security rather than causing harm or personal gain. Ethical hackers use the same tools, techniques, and mindset as attackers - reconnaissance, scanning, exploitation, privilege escalation, and persistence - but they document findings, provide remediation recommendations, and often work alongside internal security teams.

The core distinction lies in intent, authorization, and outcome. Malicious (black-hat) hackers operate without permission, typically motivated by financial profit, espionage, disruption, or ideology; their actions are illegal. Ethical hackers, by contrast, operate transparently, report all findings (even if embarrassing), and help organizations strengthen defences. This proactive approach has become essential as cybercrime costs continue to escalate globally - projected in the trillions annually - with sophisticated threats increasingly powered by AI, automation, and supply-chain attacks.

We will unpack this more in our next Newsletter. In the meantime, watch this interview by our Director, Leon Greyling, of an ethical hacker.

https://youtu.be/7B30MyBnRk8?si=UGpIYQbSqsEFLBdW

ICTS Legal Services Assessment Experiences To-date

Having conducted over 100 assessments of third-party providers to retirement funds over the past 6 months, a few patterns and lessons have emerged.

Firstly, don't panic, most providers have a reasonably good level of security in place. There are a few outliers though with their heads in the sand – we need to work with them to help improve their security and in turn that of our customers (the retirement funds).

Secondly, don't rest on your laurels....as you can see, even the biggest organisations are being targeted. And that's where the biggest lesson has been learnt. Letters of assurance are common place, particularly with the bigger providers, but unless independent audits (of standing) have been conducted then trustees must demand more transparency.

Finally, the levels (or even existence) of cyber insurance is a concern, especially given some of the stats referenced in this newsletter.

Closing Thoughts

The first half of 2026 reinforces that no sector is immune - especially when relying on third-party platforms. Proactive patching, vendor risk management, and user awareness remain critical. Stay vigilant, and we'll catch you next month with more What The Hack updates, and maybe some more byting jokes!

If you would like a gap analysis against JS2, third-party vendr assessments, 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 or when required. Past editions available on request.