ICTS
LEGAL SERVICES

Cyber news that bites back

Issue 6 • July 2026

WHAT THE HACK?

NEWS

CYBER SECURITY AND CYBER RESILIENCE INSIGHTS FROM ICTS LEGAL SERVICES

THE EVOLVING IMPERATIVE OF BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING IN THE CYBER AGE

MANAGING CYBER INCIDENTS: THE CRITICAL ROLE OF FREQUENT AND CLEAR COMMUNICATION

Dear Valued Clients and Colleagues,

Managing Cyber Incidents: The Critical Role of Frequent and Clear Communication

In the aftermath of a cyber incident, technical recovery is only half the battle. How an organisation communicates - with clients, regulators, staff, and the public - often determines the long-term reputational and operational impact. Transparent, frequent, and empathetic communication builds trust, reduces panic, limits the spread of misinformation, and demonstrates accountability.

Two recent South African examples illustrate this well.

AVBOB: A Strong Example of Proactive Communication

What stood out was how AVBOB handled communication:

- They issued clear public statements relatively quickly once the incident was confirmed.
- They published a dedicated Questions & Answers (FAQ) document on their website, directly addressing key client concerns in simple language (e.g. “Did someone hack into AVBOB’s systems?”, “What kind of information has been compromised?”, “What are you doing about it?”).
- They were transparent about what they didn’t yet know - stating that investigations were ongoing to determine whether personal information had been impacted.
- They emphasised that physical branches remained open and were operating on manual processes, reassuring clients that core services (claims, payments, funeral arrangements) were still available.
- They proactively warned clients about scam risks (fake payment links, WhatsApp messages, etc.) that often surge during outages.
- They confirmed engagement with specialist partners and notification to the Information Regulator.

In early June 2026, AVBOB (one of South Africa’s largest mutual assurance societies, specialising in funeral and life cover) suffered a cyber incident when external malicious actors compromised parts of its IT infrastructure. This led to significant disruption of its digital platforms and online services.

By maintaining a steady flow of honest updates and providing a central, authoritative source of information (the FAQ), AVBOB helped manage client anxiety and reduced the opportunity for scammers to exploit the situation. This approach is widely regarded as best practice in incident response.

The Recent PPS / Profmed Incident (June 2026)

In contrast, a more recent incident involving Profmed (a well-known medical aid scheme) highlights the challenges of third-party risk and notification.

On the evening of Wednesday, 25 June 2026, Profmed notified its members of a data security incident. The breach originated at its administrator, PPS Healthcare Administrators (PPSHA) - the fourth-largest medical scheme administrator in South Africa, serving over 200,000 clients across various schemes, including Profmed.

What happened:

An unauthorised individual gained access to certain service provider systems using compromised login credentials.

The attacker may have accessed and removed some information.

Potentially exposed data includes: member names, identity numbers, contact details, membership numbers, and scheme option information.

At this stage, it appears to be a credential-based compromise rather than a sophisticated ransomware attack or large-scale data exfiltration. Profmed and PPSHA moved relatively quickly to notify affected members once the incident was confirmed.

Effective communication during a cyber incident should be:

- Timely - Don't wait for perfect information.
- Consistent - Use one authoritative voice and central source (website/FAQ).
- Empathetic - Acknowledge client concern.
- Action-oriented - Tell people what they should do (change passwords, watch for scams, contact support).
- Regulatory compliant - Notify the Information Regulator where required.

In both cases, the organisations ultimately did the right thing by notifying affected parties. However, AVBOB's more structured and frequent communication (especially the proactive FAQ and scam warnings) stands out as a strong model for how South African financial and insurance entities should respond when things go wrong.

As cyber incidents become more frequent, the organisations that recover best will be those that treat communication as a core part of incident response - not an afterthought.

THE CYBER RESILIENCE BOARD GAME

CyberWord is a cybersecurity-themed word puzzle game combining elements of Wordle, anagrams, and riddles. Players guess cyber-related terms from clues and scrambled letters while learning key concepts.

Simple Rules

- You get 5-7 scrambled cyber words + a short clue for each.
- Unscramble the letters to reveal the real term.
- Bonus points for explaining the term in one sentence (great for discussion!) – play the game in your business to encourage.
- Difficulty levels: Easy (common terms), Medium (technical), Hard (advanced threats).

See answers at end of Newsletter.

How to Use This Game

1. Newsletter: Print or embed as an interactive section.
2. Training: Teams compete to solve fastest + explain terms.
3. Variations: Make it a timed "Cyber Escape Room" style challenge or add a Wordle-style grid for guessing letters.

PUZZLED?

Puzzle 1 (Medium Difficulty)

1. Clue: The digital version of breaking and entering.
   Scrambled: **K A C H I N G**

Answer: _____

2. Clue: Malicious software that holds your files hostage for ransom.
   Scrambled: **S R E M A W O R A N**

Answer: _____

3. Clue: A fake login page designed to steal your credentials.
   Scrambled: **G N I H S I H P**

Answer: _____

4. Clue: Two-factor's annoying but essential cousin.
   Scrambled: **F A M**

Answer: _____

5. Clue: A hidden way back into a system after initial access.
   Scrambled: **O D O R K C A B**

Answer: _____

6. Clue: The process of making data unreadable to unauthorized users.
   Scrambled: **T P N O Y R I C E N**

Answer: _____

7. Clue: A plan to keep business running during a cyber crisis.
   Scrambled: **C B P**

Answer: _____

The Evolving Imperative of Business Continuity and Disaster Recovery Planning in the Cyber Age

In an era defined by digital interdependence, a company's Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) has never been more critical. Two decades ago, these plans primarily addressed physical threats - fires, floods, earthquakes, or power failures. These events were often localised, somewhat predictable in pattern, and allowed time for manual workarounds or relocation to alternate sites. Recovery was painful but feasible with good insurance and paper-based processes.

In an era defined by digital interdependence, a company's Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) has never been more critical. Two decades ago, these plans primarily addressed physical threats - fires, floods, earthquakes, or power failures. These events were often localised, somewhat predictable in pattern, and allowed time for manual workarounds or relocation to alternate sites. Recovery was painful but feasible with good insurance and paper-based processes.

Today, the threat landscape has shifted dramatically. Cyber risks are the dominant and most pervasive danger. Sophisticated attacks such as ransomware, data breaches, Distributed Denial of Service (DDoS), and supply-chain compromises can cripple operations globally in minutes, with permanent data loss or extortion if recovery is not robust.

Why BCP/DRP Matters More Than Ever

The Shift from Physical to Digital Threats
Traditional disasters impacted physical assets and were often slower to escalate. A fire might destroy a server room, but data could potentially be reconstructed. Cyber incidents are instantaneous, malicious, and designed for maximum disruption. Ransomware frequently targets backups, while attackers exploit interconnected digital ecosystems (cloud services, third-party vendors, remote access). Global cybercrime costs are projected to reach $10.5 trillion annually, with average breach costs around $4.5 million and downtime frequently exceeding $300,000 per hour.

For South African financial institutions and retirement funds, the stakes are particularly high. Member data sensitivity, payment processing, theft of assets, and regulatory reporting mean that even short disruptions can erode trust and trigger compliance issues. The Joint Standard 2 of 2024 (Cybersecurity and Cyber Resilience), effective 1 June 2025, explicitly requires financial institutions - including retirement funds - to maintain effective recovery capabilities from cyber events as part of broader resilience requirements.

Amplified Business Impact

- Speed and Scale: Cyber attacks bypass physical barriers and affect entire digital infrastructures simultaneously.
- Regulatory Pressure: JS2, POPIA, and other frameworks demand rapid incident response and recovery. Non-compliance brings fines and reputational damage.
- Interconnected Risks: Reliance on administrators, asset managers, and fintech creates cascading failures.
- Existential Threat: Studies show a high percentage of companies suffering major data loss or prolonged outages do not survive long-term. For retirement funds, this directly impacts member outcomes and fiduciary duty.

The Dangerous Trap of Overconfidence and Inadequate Testing

- Despite the elevated threats, many organisations remain complacent. Common mindsets include "It won't happen to us," "Our IT team has it covered," or treating the BCP as a static compliance document that sits on a shelf. Staff turnover further erodes effectiveness - key personnel who understood roles and procedures leave, and new staff are not properly trained.

Testing Gaps Are the Biggest Risk

- Plans are only as good as their validation. Best practice calls for regular exercises (at least annually, plus after any major change). In reality, many conduct only superficial tabletop discussions. Full simulations, including realistic cyber scenarios (ransomware, system failover under pressure), are rare due to cost or fear of disruption. The result is false confidence - gaps are discovered only when a real incident occurs, when the cost is highest.

- Real-world examples like the 2024 CrowdStrike outage and various ransomware cases show that even sophisticated organisations suffer when change management and testing are insufficient. For SA retirement funds, this could mean inability to process benefits or report to regulators within JS2 timelines. Read more on the CrowdStrike outage here *https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages*

Moving Forward

A robust, frequently tested BCP/DRP integrated with cyber resilience is now fundamental to survival, regulatory compliance, and fulfilling fiduciary responsibilities. Treat it as a living programme: update after staff or system changes, conduct meaningful exercises – periodically and frequently, cross-train teams, and ensure board-level oversight. In the old days, surviving a fire was possible with insurance and alternate premises. Today, thriving after a cyber incident requires proactive, battle-tested resilience.

Organisations that embrace this approach not only reduce risk but build trust and competitive advantage in South Africa's financial sector.

Closing Note

As cyber threats continue to evolve in sophistication and frequency, the incidents at AVBOB and PPC/ Profmed serve as powerful reminders that technical recovery alone is never enough - clear, timely, and transparent communication is the cornerstone of effective incident management and stakeholder trust. By treating Business Continuity Planning, rigorous testing, and proactive communication as non-negotiable disciplines, South African retirement funds and financial institutions can move beyond mere compliance with Joint Standard 2 toward genuine resilience that protects member outcomes and organisational reputation.

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.

Get tested!

What The Hack Newsletter
Test. Recover. Repeat

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

Puzzle Solutions -
Don't peek until you've tried!

HACKING – Unauthorized access to systems.
RANSOMWARE – Encrypts data and demands payment.
PHISHING – Social engineering via deceptive messages.
MFA – Multi-Factor Authentication.
BACKDOOR – Secret entry point left by attackers.
ENCRYPTION – Converts data into a secure code.
BCP – Business Continuity Plan.

Bonus Challenge: Create your own scramble using a term like "ZERO TRUST" or "SUPPLY CHAIN" and share it!

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