



Cyber news that bites back
Issue 10 • October 2026

WHAT THE HACK?



NEWS

REGULATOR
AUDITS
MATERIAL
CYBER
INCIDENT
REPORTING

GLOBAL
CYBER
WATCH

SA CYBER
WATCH

THE AUDITOR COMETH. SO DID DIRE WOLF.

At about the same time that the FSCA's retirement-fund supervisory questionnaire landed on desks with a 37-question cybersecurity section, a single FICA vendor put Alexforbes, EasyEquities, and a queue of other brands on the same incident clock.



“

Pinky, are you pondering what I'm pondering?

I think so, Brain. But this time taking over the world starts with classifying a material incident in 24 hours and proving the administrator's SOC 2 is not a PDF from 2022.

WHAT THE AUTHORITIES ARE ASKING

The Authority's Retirement Fund Supervisory Questionnaire is an audit in a spreadsheet. Instructions are blunt: complete every field, do not insert or delete rows, return it as Excel, keep the original format or it may be rejected. Colour-coded Yes/No drop-downs. White cells for the fund. Comment columns for the story behind the tick.

Section 21 - tagged against Joint Standard 2 of 2024 - is the cyber chapter. It is not a policy inventory. It is a test of whether the board can show governance, strategy, identification, protection, detection, response, testing, third-party assurance and regulatory notification. The document column next to each question tells you what the supervisor will ask for next.

WHAT SECTION 21 ACTUALLY WANTS

Theme (JS2 ref)	What the fund must be able to produce
Governance (s4, s5)	Committee mandate for cyber; RACI and lines of defence; cyber in the ERM framework; board awareness training (s7.2.7); cyber duties written into providers' SLAs.
Strategy & framework (s6)	Board-approved strategy aligned to the fund's business; annual review; framework tied to ERM; independent review of the framework at least annually; metrics that are included in board packs.
Identify & protect (s7.1–7.2)	Classified processes and assets including those at third parties; inventory reviewed at least every two years; risk assessments; IAM and MFA; DLP; same security standard for administrator-held member data as for anything on the fund's own laptop.
Detect, respond, recover (s7.3–7.5)	Continuous monitoring; tested backups; defined RTO/RPO; a tested incident-response plan aligned to those objectives; a member communication plan; a written account of any incident in the period, including whether it was reported as material.
Testing & hygiene (s7.7, s8)	Vulnerability assessments; annual (or post-change) pen-tests on critical systems; scenario simulations; a remediation register; MFA on admin and member-data systems; patch SLAs; endpoint malware; third-party test assurance (SOC 2 / equivalent).
Notifications (s9) + two-pot	A materiality classification process; any FSCA notices in the period; a log of non-material events; a two-pot social-engineering risk assessment; identity checks at application and at payment.

Section 9 of JS2 is the live wire. After the fund classifies a cyber incident or information security compromise as material, it must notify the responsible authority in the form and manner the Authorities determine. Working practice from the draft Joint Communication 3 of 2025 determination: initial notice within 24 hours of classification, follow-up within 14 days, fund and 13B administrator to ITandCybernotification@fsca.co.za. That duty sits next to POPIA s22 and the Cybercrimes Act. Ticking “No incidents” while a FICA vendor is on a leak site is how questionnaires become enforcement files.

The questionnaire also asks, in the fidelity section (5.49–5.52), whether cyber-crime and social-engineering cover exists, at what rand limit, and whether that limit was set against the fund's actual risk - including the new high-volume two-pot channel. Section 21 and the insurance questions are one conversation.

The documents column is the real questionnaire

Every Section 21 row has a “Documents / Information Required” cell. That is the audit trail. If the comment says Yes and the file does not exist, the answer is No.

Minimum pack before the spreadsheet leaves the PO's desk:

Have on file	Maps to
Committee ToR covering cyber	21.1
RACI / governance extract	21.2, 21.3
Board cyber-awareness attendance	21.4, 21.18
SLA extracts - admin and managers	21.5, 21.17, 21.32
Approved strategy + last review minute	21.6, 21.7
Framework + independent review report	21.8, 21.9
Board cyber-risk pack (metrics)	21.11
Latest security risk assessment	21.14
Backup test evidence; BCP with RTO/RPO	21.20, 21.21
Incident plan + last simulation report	21.22, 21.27
Vulnerability / pen-test / remediation log	21.25, 21.26, 21.28
Materiality criteria; incident log; any FSCA notice	21.33–21.35
Two-pot fraud assessment + ID controls	21.36, 21.37

Three answers that will not survive a follow-up information request:

1. “Cyber is outsourced to the administrator.” JS2 applies to the fund. The administrator is a control (or a risk), not a substitute for board oversight, a strategy, or a notification process.

2. “We have a policy.” Item 21.6 wants a board-approved strategy aligned to the fund’s business. Item 21.9 wants an independent review of the framework at least annually. A 2019 PDF in the policy register is a No with extra steps.

3. “No incidents this period.” If a shared vendor wrote to the PO, the honest answer is Yes, with the comment column used for impact, response and whether a material-incident notice went to the FSCA.

MATERIAL CYBER INCIDENT REPORTING

Joint Notice 2 of 2026 - Determination of the Notification Template for Joint Standard 1 of 2023 and Joint Standard 2 of 2024 - was signed by the FSCA Commissioner and the PA CEO on 31 August 2026 and took effect on 1 September 2026.

What trustees of a South African retirement fund must know:



1. One-page trustee briefing

The legal duty in one sentence

Once the fund (or a provider acting for it) classifies a cyber incident or information security compromise as a material incident, the responsible authority must be notified in the form and manner the Authorities determine. That is paragraph 9 of Joint Standard 2 of 2024.



Who is in scope

The Standard applies to financial institutions as defined in JS2, including a pension fund registered under the Pension Funds Act and its providers. Trustees remain accountable for the fund even where detection, containment and first-line reporting sit with the administrator or other outsourced providers.

What “material” means

A material incident is a disruption of a business activity, process or function that has, or is likely to have, a severe and widespread impact on the fund’s operations, services to members / beneficiaries / participating employers, or the broader financial system and economy. Rand loss is only one factor. Member data compromise, inability to pay benefits, freeze of contribution processing, or a third-party outage that stops the fund can all meet the test

Working reporting clocks

Stage	When	What goes in	Channel (fund / 13B)
Initial notification	Within 24 hours of classifying the event as material	Key facts, detection method, contacts, status, Section A cyber fields	FSCA template to ITandCybernotification@fsc.co.za
Follow-up update	Within 14 days of the initial notification	Section B: disruption, member impact, loss, legal/reputational exposure, systems, vector, containment, mitigation	Same template / same mailbox
Close-out / further info	As agreed with the FSCA	Resolution, residual risk, lessons learned, control changes	Same channel plus board pack

The 24-hour clock starts on classification as material, not on first suspicion.

What JS2 does not replace

POPIA notification to the Information Regulator and affected data subjects; Cybercrimes Act reporting where a crime is suspected; any notice required by fund rules, the administration agreement or insurers; and material IT-incident notification under Joint Standard 1 of 2023 (same draft template is intended to cover both).

What the board must be able to answer

1. Who classifies materiality for an event at the administrator, actuary, asset manager, consultant or cloud provider - and in what hours?
2. Who presses “send” on the FSCA notification if the incident sits in a provider’s environment but hits fund members?
3. How is the Principal Officer / chair notified inside the first few hours, including after hours and weekends?
4. Are member-communication, POPIA and Cybercrimes tracks running in parallel with the JS2 notice?
5. Where is the last table-top test of this plan, and when is the next one?

2. Materiality prompts for a retirement fund

Classify as material (or escalate immediately for a classification call) if any of the following is true or reasonably likely:

- Benefit payments, two-pot withdrawals, death/disability claims or divorce orders cannot be processed within the fund's RTO.
- Contribution or membership files are encrypted, altered or unavailable, so participating employers cannot remit or the fund cannot allocate.
- Member, beneficiary or trustee personal information (IDs, bank details, medical, balances) is exfiltrated, published or credibly threatened.
- The member portal, call centre or trustee board pack systems are down long enough to cause widespread service failure or missed statutory deadlines.
- A ransomware or business-email-compromise event hits the administrator, consultant or a material asset manager and the fund's data or mandate is in scope.
- There is a credible risk of contagion to other funds on the same administration platform.

3. Checklist the Principal Officer can run in the first day

#	Check
---	-------

1	Incident logged with time of detection, time of PO notification, and time of materiality classification.
---	--

2	Containment status confirmed: accounts locked, malware isolated, backups verified offline.
---	--

3	Section A of the material IT/cyber template completed; sent to ITandCybernotification@fsca.co.za; sent item and attachment saved to the fund file.
---	--

4	POPIA / Cybercrimes / insurer / participating-employer notices considered in writing, even if the decision is "not yet".
---	--

5	Chair and risk committee informed; special meeting set if payments or member data are affected.
---	---

6	Member holding statement approved or consciously deferred, with reasons minuted.
---	--

7	Day-14 Section B owner and diary date assigned before the first night is over.
---	--

ASSESSMENTS UPDATE

While funds fill in Section 21, the market on the other side of the SLA is being scored. Snapshot at September 2026 across provider cyber assessments conducted by ICTS Legal Services in conjunction with the Cyber Security Institute (CSI):

Metric	September 2026
Assessments completed	101
Assessments in progress	53 - targeted completion end-October 2026
Provider categories	21 - asset management the largest cohort
Overall score (out of 5) - average	3.82
Highest / lowest overall	4.39 / 2.28
Lowest single sub-category score	1.13 - Context of the Organisation
Lowest sub-category average	3.31 - Cybersecurity Strategy and Framework



SA CYBER WATCH

September’s lesson in one line: the perimeter you do not own is still your perimeter. Funds that answered Section 21.5, 21.17 and 21.32 with “the administrator handles that” now have a worked example.

RelyComply - one vendor, many letterheads

On 8 September 2026 RelyComply, a South African FICA / AML / KYC platform, became aware of unauthorised access to systems holding customer data. It says a zero-day in a third-party application was exploited. Dire Wolf listed the firm on its leak site on 9 September, claiming 200GB from production databases and Amazon S3 - identity verification, transaction monitoring, screening and credential stores; the group’s own numbers talk of 3.57 billion rows and about 92 million rows of core customer data across 23 organisations. RelyComply reported the incident to the Information Regulator (ref SC20263150), took systems offline, rebuilt, and rotated credentials and API tokens.

Then the weekend letters started.

Institution	What they have said in public
Alexforbes	Confirmed a data-security incident at RelyComply (AML, screening, risk assessment). Preliminary view: some identity-related client information may have been accessed. Own IT, platforms and networks said to be uncompromised. Data-sharing with RelyComply suspended, then screening reinstated after forensic sign-off and credential replacement. Regulators formally notified.
EasyEquities / Purple Group	Provider confirmed access on the evening of 10 September; integration disabled 11 September. Own and parent systems: no evidence of breach; 30-day threat hunt found only blocked reconnaissance. Data in scope: name, ID, DoB, gender, nationality, residence, account number. c.2.9 million registered users; not all passed through this provider.
Satrix / Sanlam link	SatrixNOW is operated by EasyEquities and uses the same verification stack. Satrix said there is no indication SatrixNOW itself was compromised. EasyEquities is 30% owned by Sanlam Investments - the third-party path into a Sanlam-branded platform, not a claim that Sanlam’s core estate was breached.
Also in the blast radius	Peregrine Capital, Bidvest Bank, SA Home Loans. Standard Bank said it is investigating whether client data sat in the same vendor store.

MIP HOLDINGS - JUNE, STILL LEAKING IN SEPTEMBER

A separate supply-chain story. MIP Holdings, which supplies policy administration and CRM to insurers, medical schemes, lenders and pension administrators, detected a Gentlemen ransomware/extortion attack on 14 June 2026 on a third-party Jira tool and associated FTP/SFTP. MIP says core admin databases were not hit. Personal information of employees, client users and members sat in tickets, attachments and screenshots. About 45 insurer clients - roughly half of MIP's book - and in the region of 400,000 records. The Gentlemen later dumped data linked to Hollard. Hollard's line: MIP incident, not a Hollard-system breach. The National Fund for Municipal Workers has already warned members that some personal information may have been accessed via MIP. If your administrator or insurer sits on that stack, Section 21.23 and 21.34 are not theoretical. Funds have to have oversight.

Elsewhere on the Highveld

- Cartrack / Karooooo - Dire Wolf again. Attack around 26 August; leak-site claim of 500GB. Customer database in play: identity, contacts, addresses, bank details, vehicle and driving data. Information Regulator confirmed a POPIA s22 notification and is studying it. Platform restored the same day; dark-web publication confirmed 8 September.
- Hungry Lion - MeduzaLocker, the same crew that hit The Courier Guy, listed the 111-store QSR group. Ransom chatter around US\$50,000.
- Furniture Bargaining Council - Deadlock ransomware, industry payroll and member services disrupted.
- Daily Maverick's September round-up also put Bidvest Bank, Serengeti Estates and Toyota SA on the month's incident list. The pattern is not "sophisticated APT versus nation state". It is commodity ransomware plus one shared vendor.

WHAT IS ACTUALLY HAPPENING



A criminal crew ran a product. Dire Wolf's own leak-site line is the business model in one sentence - they want money, not politics. They encrypt, steal a copy, list the victim, and sell silence. Same playbook as The Gentlemen on MIP. Off-the-shelf ransomware-as-a-service, double extortion, a countdown on a Tor site. Nothing particularly sophisticated, just a run of the mill hack.

GLOBAL CYBER WATCH

August 2026 was the worst month on record for ransomware. Comparitech counted 997 attacks - about 32 every day. That is 23% more than July, and higher than the previous peak in February 2025.

Two gangs did most of the shouting: Qilin listed 157 victims; The Gentlemen (the same crew that hit MIP in South Africa) listed 107. Hospitals were hit 30% more often. Attacks on power and water companies doubled. The United States took 417 of the month's cases.

What a retirement-fund board should take from the big names:

Apollo Global Management

Criminals talked their way into a cloud login (6–10 July). They walked out with names, dates of birth, addresses and ID numbers. Large asset owners are being targeted the same way.

UK airports (MAG)

8.7 million customer records leaked from car parks, lounges, fast-track and airport Wi-Fi. Planes still flew. The lesson: the side system - not the “main” one - often holds the personal information.

McKesson / ShinyHunters

A third-party app was breached. The gang claimed huge volumes of patient records and talked about a ransom above US\$55 million. Health data is being treated the way member data is treated here.

ClOp / PTC Windchill

More than 40 companies appeared on a leak site because they all used the same product-lifecycle software - Shell, Philips, GE, Fiserv among them. One shared tool, many brands. That is the RelyComply story with a Northern Hemisphere accent.

Hungary's state treasury and a small UK power plant

Public-finance systems were hit with ransomware. A UK generator was shut for four days in an attack linked to Iran. Industrial kit is no longer “someone else's problem.”

Capita Pension Solutions (UK)

In October 2025 the UK privacy regulator fined this pensions administrator £14 million for poor security after a breach. Supervisors do fine administrators. Ours have started with a questionnaire.

Also in August, and worth a line only: Boston Scientific had a global IT outage; the Medusa gang passed 500 hospital victims; a China-linked strain of Babuk ransomware used a new hole in VMware vCenter; and phishing written with AI no longer looks like a clumsy scam letter.

None of that changes the local job. It does explain why Section 21 of the FSCA questionnaire asks whether last year's pen-test is still last year's pen-test.



Pinky: Gee, Brain, what are we going to do tonight?

Brain: The same thing we do every night. Classify the incident, notify the Authority, and make sure the administrator's third party is on the inventory. Then we take over the world.

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.

Breaking out of the box on risk management

Sources for the Watch pages: company notices and ITWeb / MyBroadband / Moneyweb / Daily Maverick reporting 13–22 September 2026; RelyComply incident page 16 September 2026; MIP Holdings POPIA notice 23 June 2026; Comparitech ransomware round-up August 2026; FSCA Joint Standard 2 of 2024 and the Retirement Fund Supervisory Questionnaire Section 21. Assessment figures from the September 2026 provider-assessment snapshot supplied with this edition.

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



BRAIN'S CLOSING BRIEF

The FSCA questionnaire is not a new standard. It is JS2 turned into a mark sheet. Section 21 is where the Authority will test whether funds noticed that September's breaches did not start inside the fund. They started with those appointed by the funds guardrails that protect civil liberties, and ultimately humanity. The debit column needs to be carefully managed.

Stay vigilant, stay resilient.

The ICTS Legal Services Team



What The Hack is published monthly or when required. Past editions available on request.
This newsletter is for information purposes only and does not constitute legal advice.