KILLSWITCH · ISSUE #18 · 18 NOV 2026

Password1, Twelve Years Later: The Test Account Nobody Removed

A 2012 test account with the password "Password1" let ransomware in. The regulator reprimanded the organisation and its IT provider.

Killswitch rating: Review every account this month

By Emmanuel Aigbehi Walstra

Password1, twelve years later

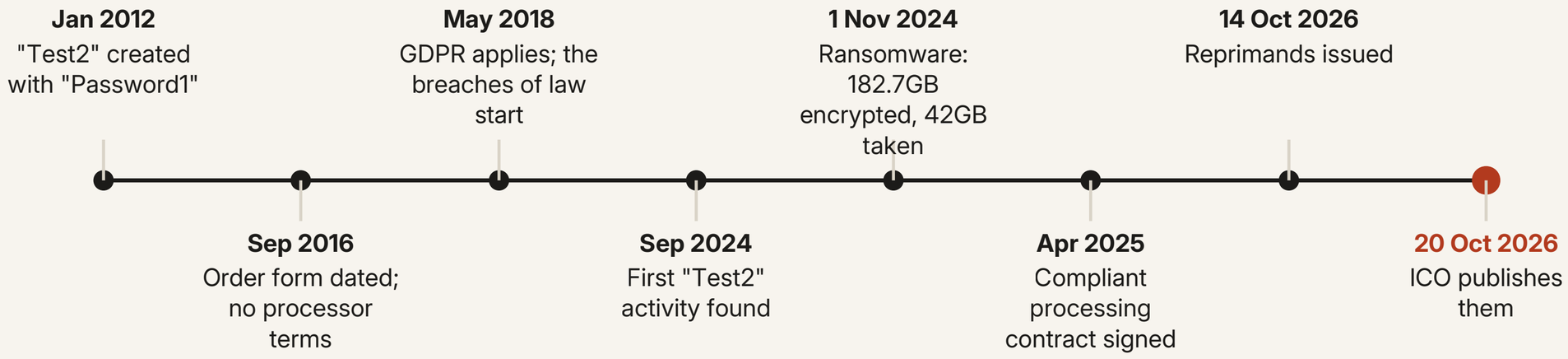
A test account created in 2012 with the password "Password1" let attackers in; ransomware followed on 1 November 2024 [1][2].

- 3,300 people affected, most of them children [1].
- The ICO reprimanded both the organisation and its IT provider. Reprimands, not fines [1].

Two reprimands, one gap

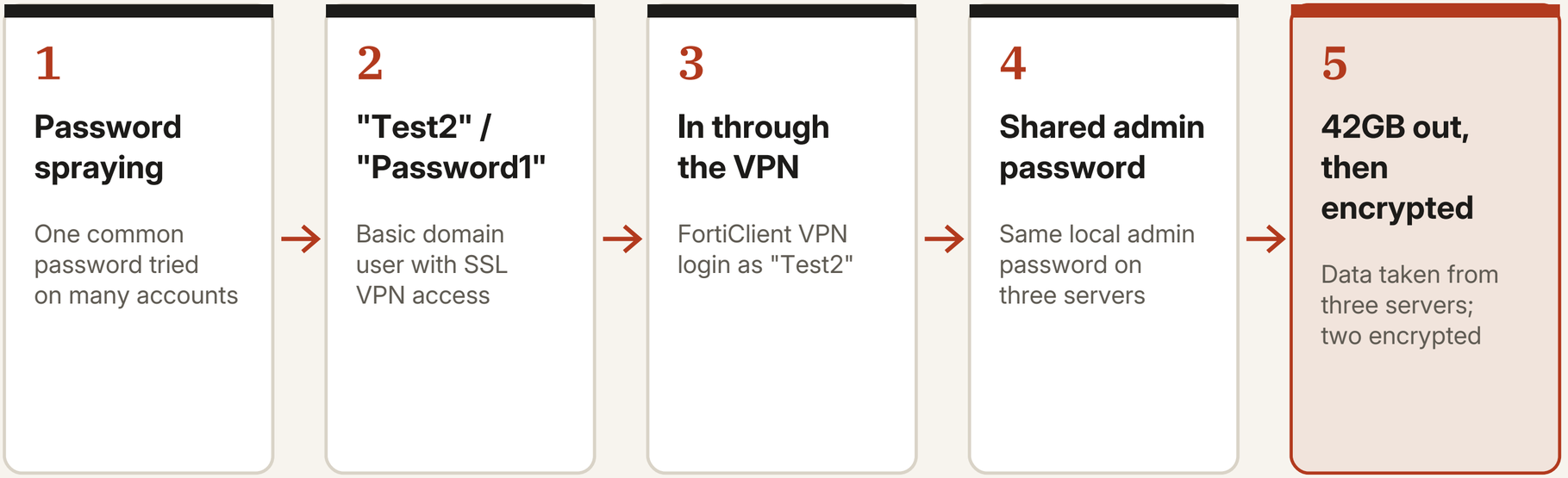
- Both breached UK GDPR Art. 32(1)(b) and (d) [1].
- Data Cymru also breached Art. 28(4): no sub-processor terms in the contract [1][3].
- The breaches of law ran six and a half years, unnoticed [2][3].
- Ogi Networks did not dispute the findings; Data Cymru accepted them [2][3].

From test account to reprimand, 2012 to 2026



ICO news release [1] and reprimands [2][3]. Earliest attacker activity per the provider's incident responder, cited by the ICO [2].

How one test account became a breach



ICO reprimand to Ogi Networks [2], citing its incident responder; ICO news release [1].

Why the password policy didn't catch it

- Data Cymru required 15-character passwords by Group Policy [3].
- "Test2" was unused and "had not logged into the domain", so it was never made to change its password [3].
- Ogi's own policy did not reach the customer's network [2].
- A policy at the next change misses accounts that never change.

The gap between two organisations

IT provider (Ogi Networks)

Created "Test2" with "Password1"
January 2012, during onboarding [2]

No audits of accounts it created
In the customer's directory [2]

Its password policy stopped at its own accounts
It could not enforce it in the customer's network [2]

Local admin passwords never reviewed
Same password for 12.5 years [2]

Customer (Data Cymru)

Controlled the network
Accounts made or removed only on its instruction [3]

Reviewed only "Domain users"
Not the full directory, not on a schedule [3]

New password rules never reached "Test2"
Unused; never prompted to meet the new password rules [3]

No Article 28 contract
A 2016 order form with no processor terms [3]

ICO findings [1][2][3]. "The responsibility for these failures did not sit with one organisation alone" [1].

The review that would have found it

- After the attack, the two reviewed every account together [3].
- It took "just over four hours" [3].
- It found eight unused accounts, one with admin rights [3].
- Before: reviews covered only "Domain users", not on a schedule [3].

Six controls the ICO lists

1 Remove what is not needed

Test, dormant and former-user accounts

2 Block weak passwords

A deny list that rejects "Password1"

3 MFA on remote access

By default, for every VPN account

4 Audit everything

All accounts, permissions and groups, not a subset

5 No shared admin passwords

Unique credentials for each system

6 Write it in the contract

How controls are delivered, monitored and audited

The ICO's "lessons for organisations" [1], shortened. Order and wording ours.

Where this lives in your frameworks

Accounts	A.5.16, A.5.18, A.8.2 · Evidence: full directory review, signed off, on a schedule
Passwords and MFA	A.5.17, A.8.5 · Evidence: deny list, MFA on every remote path, unique local admin
Suppliers	A.5.19, A.5.20, A.5.22 · UK GDPR Art. 28 · Evidence: processor contract with an account RACI
Test the controls	A.5.35, A.5.36 · UK GDPR Art. 32(1)(d) · Evidence: review results and fixes

Killswitch's own mapping. Check ISO titles against your licensed copy.

UK GDPR Art. 28, 32 [1][2][3] · ISO/IEC 27001:2022 [6]. Killswitch mapping.

10 · STILL OPEN

What we don't know yet

- Who the attackers were: not named [1][2][3].
- No evidence the data was published, as of the reprimand [3].
- Parts of both reprimands are redacted [2][3].
- ICO pages read from Internet Archive copies of 20 to 23 Oct [1][2][3].

This week

- Export the full directory and review every account with its owner.
- Disable test and long-unused accounts.
- Ban "Password1" and its cousins.
- MFA on every remote access path.
- Unique local admin passwords.
- An account RACI in the IT provider contract.

Sources

[1] ICO: "'Password1' is not an appropriate password": Two Welsh organisations reprimanded after cyber-attack exposed children's information (20 Oct 2026; read via the Internet Archive copy of 23 Oct 2026)

[2] ICO: Reprimand to Ogi Networks Limited, Articles 32(1)(b) and (d) UK GDPR (dated 14 Oct 2026; PDF read via the Internet Archive copy of 22 Oct 2026)

[3] ICO: Reprimand to the Local Government Data Unit – Wales (Data Cymru), Articles 28(4), 32(1)(b) and (d) UK GDPR (dated 14 Oct 2026; PDF read via the Internet Archive copy of 20 Oct 2026)

[4] ICO: Enforcement action, Ogi Networks Limited (14 Oct 2026; read via the Internet Archive copy of 20 Oct 2026)

[5] ICO: Enforcement action, Local Government Data Unit – Wales (14 Oct 2026; read via the Internet Archive copy of 20 Oct 2026)

[6] ISO/IEC 27001:2022 Information security management systems

[7] NIS2 Directive (EU) 2022/2555, Article 21

Facts are from the ICO's news release and its two reprimands, dated 14 Oct 2026 and published 20 Oct 2026. The ICO's site refused our requests on 10 Nov 2026, so all three were read from Internet Archive copies. The framework mapping, the self-test and the tabletop are Killswitch's own.

FROM THE PUBLISHERS OF KILLSWITCH

Know every account, who owns it, and who removes it

GRCOMPLIANCE

Keep an access-review register and supplier contracts in one place, link the evidence, and map controls to ISO 27001 and UK GDPR.

Try the live demo →

demo.grcompliance.com

Self-host free: github.com/Sectutor/GRCompliance-Core

SECTUTOR

Security and GRC books, training and audit kits.

sectutor.com

Emmanuel Aigbehi Walstra is a CISO who also serves as a virtual CISO (vCISO) for several organisations, with 30+ years in cybersecurity, 10,000+ people trained, and author of the CCSP Excellence books.