

The Data Governance Mandate: Cybersecurity in Private Market Infrastructure

Securing the Trade.

Key takeaways

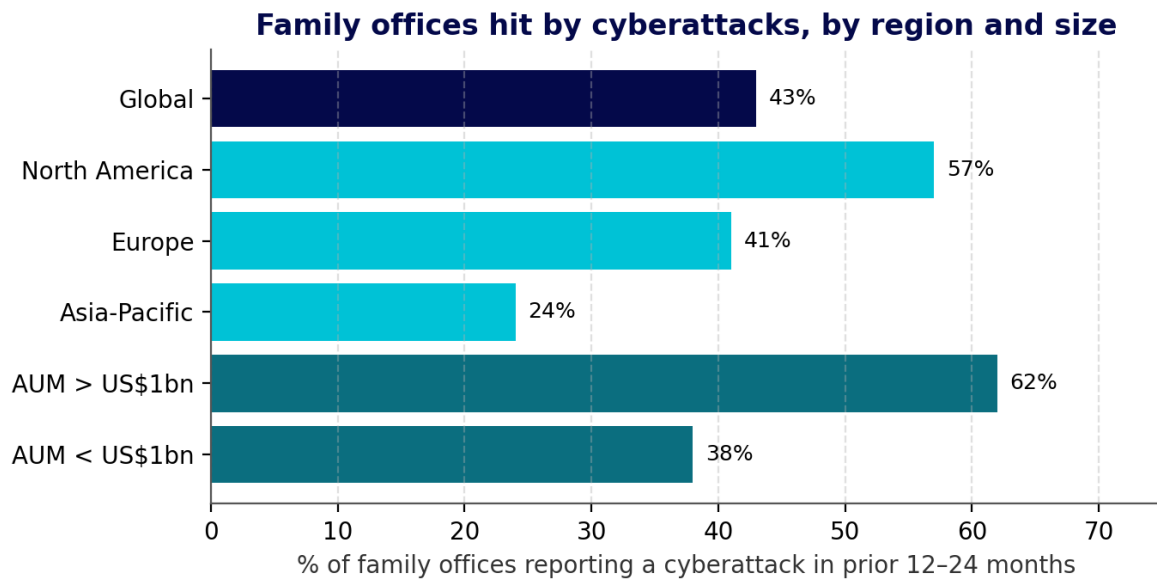
- 43% of family offices globally reported a cyberattack in the prior 12–24 months, rising to 62% among offices with more than US\$1bn in assets (Deloitte Private).
- Nearly one-third of family offices had no cyber incident response plan.
- Private-share markets are a particular target for impersonation and payment fraud, to the point that issuers now publish their own investor warnings.

Family offices have long been attractive targets for cybercriminals. They hold substantial liquid assets, often run lean teams, and depend on a network of banks, custodians and advisers. As more of them trade directly in private-company secondaries, which involve sensitive capitalisation-table data, beneficial-ownership information and large wire transfers, the security of the surrounding infrastructure has become a governance question rather than a purely technical one.

The scale of the threat

Deloitte Private's Family Office Cybersecurity Report found that 43% of family offices worldwide had experienced a cyberattack in the preceding 12 to 24 months, and a quarter had experienced three or more [1]. Exposure varied by region and rose with size: 57% in North America, 41% in Europe and 24% in Asia-Pacific, and 62% among offices managing more than US\$1 billion [1]. Phishing was the most common attack vector, reported by 93% of victims, and 31% of family offices had no incident response plan [1].

Figure 1: Share of family offices reporting a cyberattack in the prior 12–24 months



Source: Deloitte Private, *The Family Office Cybersecurity Report (2024)* [1]. Chart: Argent Bluebook.

The wider family-enterprise picture is similar. Deloitte's 2026 study of 1,587 family businesses found that 74% had faced at least one cyberattack in the past two years, and only 43% described their cybersecurity strategy as robust [2].

From IT checklist to board agenda

Industry commentary reflects the shift. Landytech's review of family-office priorities for 2026 describes cyber risk as having moved onto the board agenda, and highlights data governance: clear data ownership, separated data environments where possible, and the ability to extract data cleanly when changing providers [3]. J.P. Morgan Private Bank's 2026 Global Family Office Report adds context. Geopolitics is now the most frequently cited risk, named by 64% of family offices, and competition for talent is pushing operating costs higher [4]. Both pressures make lean offices more reliant on external platforms.

Why private-share transactions attract fraud

Secondary trades in late-stage private companies combine several risk factors: strong demand for scarce shares, limited public information, bespoke documentation and settlement by wire transfer. That combination creates room for impersonation. In May 2026, Anthropic published an investor warning that listed red flags including unsolicited offers of its stock, claims of exclusive or time-limited access, requests for payment by cryptocurrency or wire, and claims to have found a way around its transfer restrictions. It added that it does not issue stock certificates to the public [5]. The warning is company-specific, but the pattern applies more broadly: where investor demand exceeds legitimate supply, illegitimate supply tends to appear.

What institutional-grade infrastructure looks like

When family offices assess an intermediary, the questions increasingly mirror those they put to banks and custodians. Common areas of review include:

- **Identity and access:** multi-factor authentication, role-based permissions, and audit logs showing who viewed which documents and when.
- **Payment integrity:** independent call-back verification of wire instructions, escrow or delivery-versus-payment arrangements, and segregation of client money.
- **Data governance:** where data is hosted, who can access it, how long it is retained, and whether it can be exported cleanly.
- **Issuer verification:** evidence that a transfer has been approved and recorded by the issuer or its transfer agent.
- **Independent assurance:** third-party security attestations and regular penetration testing.

Trust as infrastructure

In a market where the asset is an entry on a private company's share register, the integrity of the data is the foundation of the asset. That data covers who owns what, who approved what, and where the money went. Security is not a feature added on top of a secondary trade; it is part of what makes the trade valid.

RELATED READING IN THIS SERIES

Market Lens No. 5 · Institutional Due Diligence · 20 May 2026

Market Lens No. 6 · Structured Exposure and Transfer Restrictions · 27 May 2026

References

- [1] Deloitte Private, "The Family Office Cybersecurity Report," Family Office Insights Series (Global Edition), 2024. <https://www.deloitte.com/global/en/services/deloitte-private/research/family-office-cybersecurity-report.html>
- [2] Deloitte Private, "Family business cybersecurity," 29 January 2026. <https://www.deloitte.com/global/en/services/deloitte-private/perspectives/family-business-cybersecurity.html>
- [3] Landytech, "The Top 10 Family Office Trends in 2026," 15 January 2026. <https://www.landytech.com/blog/family-office-trends>
- [4] J.P. Morgan Private Bank, "J.P. Morgan Private Bank Releases 2026 Global Family Office Report," press release, 2 February 2026. <https://www.prnewswire.com/news-releases/jp-morgan-private-bank-releases-2026-global-family-office-report-302676012.html>
- [5] Quartz, "Anthropic warns unauthorized stock sales are void," 15 May 2026. <https://qz.com/anthropic-unauthorized-stock-sales-void-warning-051526>

DISCLAIMER

This article is published by Argent Markets, a technology platform, for general informational purposes only. It does not constitute investment, legal, accounting or tax advice, and it is not an offer to sell, a solicitation of an offer to buy, or a recommendation of any security in any jurisdiction.

Investing in privately held assets is speculative and illiquid and involves the risk of loss. Argent conducts no due diligence on, and makes no representation regarding, any target company's transfer restrictions, rights of first refusal, board consent or veto rights. Parties transact at their own risk and are advised to obtain independent legal advice.

All figures derive from press reports, regulatory disclosures, or third-party data, as fully cited.