

Family Office Insights

Cybersecurity: Managing Cyber-risk Across the Family Office Ecosystem

October 2026

This article is the second instalment of a two-part series on managing AI and cyber risks in the Family Office. Part I on managing AI risks can be [read here](#).

As technology evolves, family offices occupy a unique and increasingly exposed position in the cyberthreat landscape. They manage substantial wealth, sensitive personal data, financial data and operate in lean, high-trust structures where data moves constantly between trusted advisors and the families. This makes family offices high-value targets for cyber-criminals and, even with strong internal security controls, compromised supplier systems and services can still result in serious breaches.

Evolving threat landscape

The cyberthreat landscape has evolved considerably in recent years. Attackers have developed increasingly offensive capabilities, moving away from opportunistic attacks towards targeted, intelligence-led attacks directed at high-value structures. Advances in artificial intelligence (AI) have further accelerated cyber-offense capabilities, enabling attackers to automate reconnaissance, engineer adversarial attacks, generate highly personalised phishing communications and deploy malicious code at scale and speed. With a tightening regulatory environment and layered multijurisdictional requirements, the reputational and financial costs of a breach are likely to be significant.

Vulnerabilities unique to family offices

- **Trust dynamic** – One of the greatest strengths of family offices is that they operate on deep personal trust that exists between principals, advisors, family members and staff. However, this strength is also an exploitable vulnerability for modern attack techniques. Attackers can now convincingly impersonate a trusted individual through voice cloning and other realistic deepfakes.
- **Blurred professional and IT environments** – Many family offices may already have adopted reasonably robust cybersecurity controls across their core IT infrastructure. However, potentially vulnerable external entry points into that infrastructure may exist. For instance, family members and staff routinely use personal devices, home networks, non-approved applications and other software, as well as personal email addresses for business purposes. If there are no security controls or restrictions in place for this extended environment, the attack surface expands significantly.

- **Public visibility** – Family offices and family members often maintain a degree of public visibility through philanthropic activity, board memberships, media coverage and social media presence. This publicly available information can inadvertently provide sophisticated attackers with a rich source of intelligence, which can be used to craft convincing campaigns before an attack is launched.
- **Different user profiles** – Family offices are also distinctive because their principal users frequently have a wide range of relationships with technology. Some may be active across digital platforms, while others may engage with them more selectively or rarely at all. This can create an unpredictable security profile. Those with a digital presence may inadvertently expose personal and family information, and others that are less familiar with digital channels may be more susceptible to social engineering attacks. Managing cyber-risk across the family office therefore requires a risk management approach that is sensitive to the diversity of the user profile.

Managing cyber-risk in the family office

- **Map the ecosystem** – Within the family office ecosystem, sensitive data constantly flows between advisors, accountants, banks, wealth managers, property managers and other external service providers, as well as across an array of IT networks and cloud and online services. Family members themselves hold large amounts of sensitive data on their personal networks and devices. Given the increasing sophistication of cyber-attackers and their attack methodologies, this complex chain and the data flowing across it should be carefully mapped, so that access points and technical and organizational vulnerabilities can be identified.

- **Vendor due diligence** – Not all third-party relationships carry the same level of risk, and a proportionate approach to the vendor due diligence should reflect this. Those with access to the most sensitive data warrant most rigorous scrutiny. At a minimum, family offices should be conducting appropriate diligence on prospective vendors that will have access to sensitive data and other information, to ensure they have appropriate security measures in place, including in relation to breach detection and incident response. Existing vendors should also be subject to regular diligence, to ensure standards are maintained.
- **Contractual protections** – Vendor due diligence only goes so far if vendor contracts are weak or ineffectual. Family offices should ensure that all agreements with third parties that have access to their data and other sensitive information include robust confidentiality provisions, a data processing agreement compliant with applicable data protection laws, clear obligations around security standards and a requirement to promptly notify the family office and cooperate with it in the event of any breach. Where appropriate, contracts should also include the right to audit the vendor's security arrangements and practices.
- **Incident response** – An effective and well-rehearsed incident response plan is an essential component of any credible cybersecurity framework, and one that should be stress-tested before it is needed rather than drafted in the aftermath of an attack. The plan should cover all aspects of incident response management and remediation. Key elements will include which team members should be involved in managing any breach and their roles and responsibilities, when and how internal escalation is required, when and how external specialists such as breach counsel and digital forensics consultants should be engaged, containment, eradication and recovery procedures, evidence handling requirements and regulatory compliance requirements, including in relation to notifications and relevant timelines, as well as internal and external communication protocols.
- **AI as a defensive tool** – While AI is materially accelerating the offensive capabilities available to attackers, it is also increasingly being deployed for cyberdefense. AI-enabled security tools can monitor network activity and identify anomalies, especially those engineered by AI itself, that would be difficult to detect through human oversight alone. When aligned with responsible AI governance practices, AI solutions deployed to strengthen a family office's cybersecurity posture can serve as a meaningful force multiplier. It can enhance detection capabilities, improve response times and support more consistent and scalable security controls without displacing the need for human judgment and oversight.



Conclusion

Cyberthreats are growing in sophistication, and they extend well beyond the boundaries of any single organisation's internal controls and owned infrastructure. A serious breach affecting a family office can easily result from a combination of weak processes, poor vendor diligence and undetected technical or organizational vulnerabilities, rather than sustained and significant attacker effort or a single catastrophic security failure.

Against this backdrop, managing cyber-risk requires a broader, more integrated approach; one that considers not only internal systems, but the full ecosystem of people, processes and external dependencies through which sensitive information flows. Family offices that adopt a structured and proportionate approach to identifying vulnerabilities, strengthening controls and enhancing preparedness will be better positioned to manage risk in an environment where both the threats and their potential consequences continue to evolve and increase dramatically.

Contacts



David Naylor
Partner, London
M +44 792 047 9619
david.naylor@squirepb.com



Uzma Chaudhry
Associate, London
T +44 20 7655 1330
uzma.chaudhry@squirepb.com