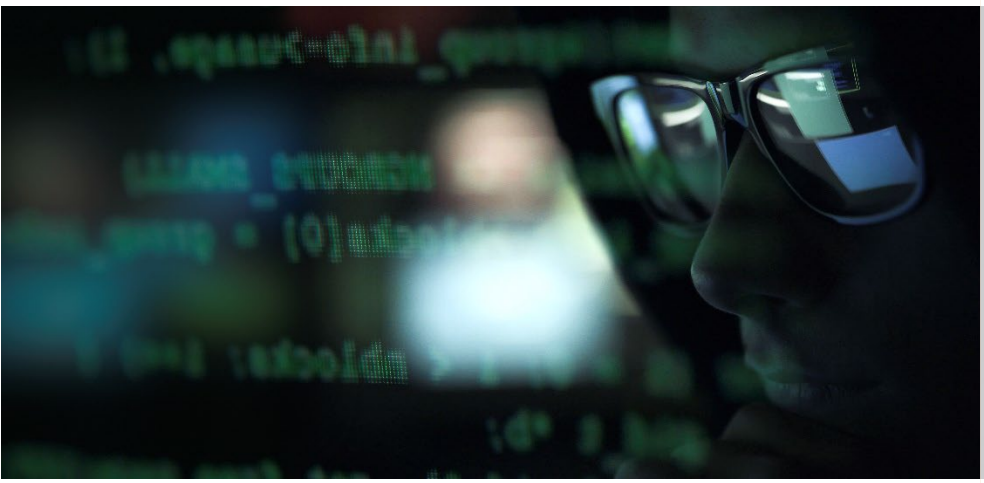
Global Insights

Cybersecurity Risks in Family Offices



Remo Stebler

Initcon Schweiz GmbH

11.06.2025

contact@initcon.ch

INITCON

Summary

Family offices are increasingly in the crosshairs of cybercriminals. These organizations, comparable with banks, operate with lean teams and less formal security controls, making them "soft but lucrative targets" for hackers. A recent global survey found that **43% of family offices experienced a cyberattack in the past two years**.[1] In North America, over half (57%) of family offices reported an attack, compared to 41% in Europe and 24% in Asia, indicating higher exposure in the US and other Western markets [2]. In Switzerland, a major hub for wealth management, cyber incidents are on the rise across the board in all sectors, with reported attacks doubling in 2024 [3]. This escalating threat landscape has made cybersecurity a top-tier risk for family offices worldwide.

Despite growing awareness, many family offices remain underprepared against cyber attacks. A Deloitte family office study notes that **nearly one-third have *no* incident response plan (ICP)**, and only 26% describe their plan as "robust" [1] [2]. Less than half have dedicated cybersecurity controls in place [4]. In one North American survey, **79% of family offices acknowledged cyber risks are increasing,** yet less than one-third have well-developed cyber risk management processes, and only 29% consider their staff training sufficient. The result is a sizable gap between rising threats and current defense. Family offices' combination of **substantial assets, sensitive data, and often informal security** makes them uniquely attractive targets. Attackers seek not only financial gain, but also sensitive personal information or even leverage for extortion and reputational damage.

Family offices, whether serving one or multiple families, must strengthen their cybersecurity to match their financial influence; it is their fiduciary duty . This report outlines key cyber threats, real-world incidents, and best practices across governance, technical safeguards, and staff awareness to help protect client wealth and privacy.

With over 25 years of experience in European family offices, including C-level and board positions, I have led a wide range of projects across operations and technology. These include process digitisation, advanced analytics, security architecture, infrastructure design, investment platforms, and data protection. Cybersecurity has been a central focus since I first entered the family office space as a consultant, informed by experience on both sides of the fence, and it remains a priority today. This report is therefore not only based case studies but reflects as well my own experience concerning cybersecurity in family offices.

Remo Stebler

Initcon (Schweiz) GmbH
Remo Stebler | LinkedIn
https://www.initcon.ch

The Cyber Threat Landscape for Family Offices

Family offices today face the risk of cyber threats once aimed primarily at large financial institutions. As banks and major firms have hardened their defences, attackers have turned to "softer targets". That means organisations with valuable assets but weaker security [5]. Family offices fit this profile: they control *significant wealth* and confidential data, yet often have small staffs and minimal IT teams. *"Family offices…have become lucrative targets for hackers,"* as one CNBC report put it [6]. In fact, **cyberattacks on family offices have become almost commonplace**. Deloitte's 2024 Family Office Cyber Report found 43% of family offices globally had a cyber incident in the prior two years, and half of those suffered **three or more** breaches [7] [2]. Notably, larger family offices (those managing >$1B) are more likely to be attacked (62% reporting attacks) than smaller ones (38%), and experience more frequent recurring attacks [1] . This suggests that as wealth and visibility grow, so does threat exposure.

Regional perspectives: Geography influences risk levels. North American family offices appear hardest hit, with 57% reporting cyberattacks (vs. 41% in Europe). One reason may be the complex digital footprint and wealth concentration in the US [1]. Europe's family offices face serious threats as well, though some may benefit from stricter data protection regimes and security awareness in financial centres. Switzerland, home to many family offices and private banks, exemplifies the broader trend: the Swiss Federal Office for Cyber Security reported that **cyber incidents doubled in the first half of 2024**, with an incident now reported every 8.5 minutes [3]. While many reported Swiss cases involve fraud targeting individuals (e.g. phone scams and parcel-delivery phishing) [3] , such attacks can easily entangle family office staff or principals, given the intermingling of personal and professional spheres.

Single-Family vs. Multi-Family Offices: Both SFOs and MFOs face similar cyber threats, but their risk management approaches can differ.

Single-Family Offices (serving one ultra-wealthy family) often have highly personalized operations with deep trust among a small team. However, this intimacy can breed security gaps: SFOs may rely on legacy systems and "informal infrastructures" that haven't kept pace with modern threats [8]. They might underinvest in cybersecurity due to cost or a false sense of obscurity.

By contrast, **Multi-Family Offices** (serving multiple families) tend to operate more like professional financial firms and may implement broader controls. They often have to meet regulatory standards and client expectations akin to private banks. Yet, MFOs hold *aggregate* sensitive data from *multiple clients*, making them rich targets. In practice, no structure is immune – wealth aggregators of any size attract cybercrime. A Campden Wealth study noted North American family offices average ~USD 2B in assets yet spend only ~USD 48'000 on cybersecurity annually, indicating a widespread resource mismatch [9].

Whether SFO or MFO, the lean staffing is a common challenge: one Wharton survey showed an average of just 4–5 IT professionals per family office, often with fewer than one dedicated cybersecurity specialist [10]. Most family offices must therefore **outsource or consult external experts** for cybersecurity needs, as their in-house capacity is limited.

Rising awareness, but slow action: Cybersecurity now tops the risk agenda for many families. 22% of family offices in a global survey cited cyber risk as a top concern [11]. High-profile incidents and warnings have spurred awareness. For example, the FBI and Europol have highlighted the surge in ransomware and sophisticated fraud targeting wealthy individuals [11]. Family office principals are increasingly realizing that a cyber breach could mean *not just financial loss, but also personal exposure* of private investments, identities, or even physical security risks. As one U.S.

family office CEO put it, *"Typically, cyber criminals go after low-hanging fruit, so the less you do, the more likely you will be a target… If you do not spend the money [on cybersecurity] and something happens, you can experience a huge loss"* [1]. Unfortunately, converting awareness into action has lagged. Surveys indicate that **31% of family offices still lack a cyber incident response plan**, and many have not conducted any basic cybersecurity audits or training [1]. This gap presents an urgent governance issue: without proactive measures, family offices remain one breach away from potentially devastating consequences. The next section examines those consequences by looking at the specific threat types and real incidents that have impacted family offices.

Key Cyber Threats and Notable Incidents

Family offices face a spectrum of cyber threats similar to those confronting large corporations, but often with **higher stakes due to the personal nature of the data and the reputational sensitivity**. Below are the most pertinent threat vectors, with real-world examples and case insights:

- **Phishing and Business Email Compromise (BEC):** *Phishing* is the most ubiquitous threat to family offices, serving as a gateway for many larger attacks. In fact, **93% of cyberattacks on family offices involve phishing emails** [1] [11]. Attackers craft legitimate-looking messages to trick recipients into clicking malicious links or divulging credentials. A common scenario is BEC, where fraudsters impersonate a family member or executive via a spoofed email. For example, a bad actor might email a family office controller *pretending to be the principal*, urgently requesting a $150,000 wire transfer, and if staff aren't trained to verify requests, they may execute the transfer before anyone realizes it was fake [5]. Such schemes have succeeded in stealing millions from family offices. (One survey cited a single BEC incident costing a family office over **$10 million** in losses). [9] The prevalence of phishing means that *constant vigilance* is required: clicking the wrong email link can not only leak passwords but also install malware or open the door to further intrusion. As Deloitte experts warn, a phishing email is often the **opening act of a ransomware campaign.** The clicked link or attachment can quietly deploy ransomware in the network [11]. Family offices, where email is a primary mode of doing business, must treat every unexpected message or funds request with scepticism and verification protocols. However, the example mentioned is not solely a cybersecurity issue. If robust approval processes were in place, such payments would not be executed, even in the event of a cyberattack. This illustrates that both security and governance need to be implemented at multiple levels.

- **Ransomware and Extortion:** Ransomware attacks, where hackers encrypt a firm's data and demand payment for its release, have hit family offices with increasing frequency and severity. While ransomware incidents at big public companies grab headlines, *"they also target family offices"*, emphasizes Deloitte's cyber risk leader [11]. Many family offices mistakenly think *"I'm just a small office, not a target"* – absolutely not true, as ransomware groups specifically seek out organizations with valuable data and an ability to pay [1]. Family offices often possess sensitive financial records, investment plans, and personal info (trusts, account numbers, private communications). If leaked, such data could be ruinous, causing financial fraud, public embarrassment, or legal liabilities [12]. Attackers know this and increasingly execute "double-extortion" tactics: before locking files, they *steal* confidential data and threaten to publish it unless paid [12]. One U.S. family office fell victim to such an attack and was locked out of its servers for 10 days, ultimately paying **$500,000 in ransom** to restore access [13]. Sadly, this is not uncommon. More than half of ransomware-hit family offices end up paying the ransom [12], often as a last resort to regain their data or keep sensitive information private. The **impact** of a ransomware breach can be crippling: operations halted for days, hefty recovery costs, and potentially

permanent data loss even after decryption. It's truly a scenario of *"pay up or shut down."* Moreover, paying a ransom is no guarantee. Criminals may take the money and still leak or destroy data. Family offices must therefore focus on **prevention and response readiness** (e.g. reliable data backups, incident drills) to avoid ever being cornered into such an impossible choice.

- **Social Engineering and Impersonation Scams:** Beyond email phishing, attackers are leveraging advanced *social engineering* to exploit the trust inherent in family offices. This includes phone-based scams (vishing), text message phishing (smishing), and even emerging threats like deepfakes. In one noted tactic, criminals use AI to mimic the voice of a family member in distress, calling a staffer to urgently wire money; a high-tech twist on impersonation fraud [10]. Family offices also report attempts at **social media hijacking**: hackers taking over a principal's social media account to trick the office or business partners (for instance, to announce a fake investment that manipulates stock prices) [4]. These ploys prey on human nature: urgency, fear, curiosity**,** rather than technical exploits. For example, the Swiss cyber incident data shows phone scammers posing as authorities convinced victims to install remote-access software, leading to bank theft [3]; such tactics could just as easily fool an untrained executive assistant. Social engineering extends to physical realm too: attackers might research family details via public sources or even tailgate into office premises by pretending to be IT repairmen. The *human factor* is often the weakest link. One family office advisory noted that *"families are porous"* – with many relatives, staff, devices, and homes in play, there are ample avenues for social engineering if proper security culture is not in place [9]. The consequences range from unauthorized funds transfers to sensitive info inadvertently disclosed to hostile actors. Education and verification protocols are key defences here: staff should be trained to double-check identities (using known contacts or secondary channels) before acting on any unusual request, no matter who it appears to come from.

- **Insider Threats:** Uncomfortable as it may be, some threats originate *inside* the family office. Insider threats involve individuals with legitimate access: employees, former staff, contractors, even family members, who intentionally or accidentally compromise security. PwC experts note this is one of the **primary attack avenues** in family offices [14]. An insider could be malicious (e.g. a disgruntled staffer siphoning confidential data for personal gain or revenge) *or* simply negligent (e.g. an employee falls for a phishing email, unwittingly giving hackers a foothold) [14]. In fact, many breaches attributed to "insiders" are actually well-meaning employees duped by external attackers [14] . Family offices are often tight-knit groups, so there can be a false sense of immunity: *"we trust our people."* However, factors like remote work, lack of background checks, and generally informal security policies amplify insider risks in family offices [8]. For example, a long-time office IT consultant might retain VPN access after their contract ends, or a family member might download sensitive reports onto a personal device with weak safeguards. If those credentials or devices get compromised, the breach is coming from "inside" the network. There have been cases (usually kept discreet) of family office employees caught snooping into trust documents or client data without authorization**.** Sometimes out of curiosity, other times with intent to leak or sell information. And consider that a single careless act (like one staffer using an easy password or losing an unencrypted laptop) can open the door to attackers. Traditional security controls often focus outward and may fail to detect internal misuse or data exfiltration. Thus, mitigating insider threats requires a mix of *technical controls* (access monitoring, least privilege principles, data loss prevention tools) and *cultural measures* (staff vetting, clear policies, fostering an environment where employees understand security is everyone's responsibility).

- **Third-Party and Supply Chain Attacks:** Family offices typically rely on **external**

vendors and advisors for many services: IT support providers, software vendors, accountants, custodians, even contractors managing physical premises. These third parties can introduce vulnerabilities if not properly managed. Cybercriminals often target smaller vendors as a backdoor into higher-value targets. The classic example being hackers breaching a HVAC (Heating, ventilation, and air conditioning) maintenance contractor to ultimately penetrate a retailer's network (as happened in the Target breach). Family offices are similarly exposed: *"Organizations are increasingly reliant on third-party providers… often sharing sensitive information with them or allowing them network access,"* a PwC specialist warns [14]. If, say, an external IT support firm that remote-manages a family office network is compromised, attackers could hop into the family office systems. Even vendors considered low-risk might inadvertently have access to the internal Wi-Fi or sensitive facilities, which hackers can exploit. Additionally, many family offices use cloud-based software; a breach at the software provider could expose **multiple family offices' data simultaneously**. Supply chain attacks have been on the rise globally: for instance, the **SolarWinds incident** where attackers infected a widely used IT management tool, affecting thousands of organizations downstream (the kind of tool a family office might use via a MSP). In the family office context, even law firms or concierge services might hold confidential family data that, if breached, would impact the family. A recent industry report noted that one in three family offices that suffered a cyberattack traced the source to a **third-party weakness** [1]. Managing this risk requires robust vendor due diligence, contractual security requirements, and monitoring of third-party access. Many family offices are now, for example, including cyber breach notification clauses in contracts with key service providers, ensuring they will be alerted promptly if a vendor's systems are compromised [15]. Ultimately, a family office's security is only as strong as its weakest linked partner.

- **Other Emerging Threats (Espionage and Physical Security):** Family offices, especially those of prominent business leaders or politically connected families, may also face more specialized threats. **Cyber espionage** is a concern if the family office's data could be valuable for insider trading or political leverage. For example, if a family office has significant holdings in public companies or involvement in sensitive industries, nation-state hackers or rival market players might target them to glean non-public information [4]. There have been reports of family offices being spied on by spyware or having their emails monitored as indirect avenues to get to a billionaire principal or a high-ranking former politician. Additionally, cyber-enabled physical threats are an evolving risk: affluent families increasingly use smart home technologies, private jets, yachts, and cars that are Internet-connected. Hackers have demonstrated the ability to exploit IoT vulnerabilities – from taking over smart thermostats to potentially disabling automotive systems. A Deloitte overview flagged that attackers could target connected devices in homes or vehicles of ultra-wealthy families (for instance, hacking into a yacht's navigation or a home CCTV system) [4]. The motive might be stalking, theft, kidnapping, or just harassment. While such scenarios are rarer than financial crimes, they underscore that family offices must secure not only traditional IT systems but also the broader digital ecosystem around the family.

The consequences of these threats materializing can be severe. Family offices have suffered large financial losses, as noted. But beyond direct money loss, the **exposure of sensitive data** is perhaps the biggest nightmare. Consider the reputational fallout if a family office's confidential files were dumped online: investment strategies, private communications, family identities, philanthropic donations, even personal photographs could all be leaked. One needs only recall the "Panama Papers" leak (though from a law firm, not a family office) to imagine the reputational damage if a family's financial secrets become public.) According to industry experts and cybersecurity consultants, there have been incidents, often not publicly attributed, where

European family offices have had confidential data posted online in the darknet after refusing to pay ransom. These cases are typically not disclosed to protect the families involved. Another possible impact is **downtime.** if a family office's systems are locked or impaired, the family could lose access to critical information needed for investments or bill payments for days or weeks [12]. In one lawsuit-revealed case, a ransomware attack on a law firm caused over 90 days of operational downtime and hundreds of thousands in recovery costs (plus reputational harm with banks and partners). [16]

These examples reinforce that cyberattacks on family offices are not hypothetical; they are *occurring regularly* globally. The imperative is clear: family offices must take proactive steps to defend against these threats and be ready to respond when (not if) an incident occurs.

Strategic Cyber Risk Management for Family Offices

Family offices can significantly bolster their cyber resilience by adopting a multi-pronged, governance-driven security strategy. The following are practical recommendations and best practices, distilled from industry reports, case lessons, and experiences over the years, tailored for the unique context of family offices. These measures aim to provide clear, actionable steps for the management and family office boards to implement:

- **Establish Governance and Incident Response Frameworks**: Treat cybersecurity as a formal business risk, not an ad-hoc IT issue. Family offices should develop a **written cybersecurity policy and an Incident Response Plan** (IRP) if they haven't already. Alarmingly, nearly one-third of family offices lack an IRP, a gap that needs immediate fixing [1]. An IRP outlines roles, communication protocols, and recovery steps when a breach occurs. It should be approved by leadership and updated regularly. In tandem, leadership should define a governance structure for cyber risk: assign clear responsibility (e.g. a designated security officer or committee) and ensure periodic reporting to principals or the board. *"Do you have a broad cybersecurity program? Do you have someone…that is a dedicated subject matter expert on cyber security? What we're finding is many do not,"* notes Deloitte's Tiffany Kleemann [11]. Remedy this by appointing a cybersecurity lead; whether an internal CISO or an external advisor, to own the strategy. Governance also means identifying what regulations apply (especially for MFOs in finance hubs) and aligning with frameworks like NIST or ISO 27001 for best practices. Crucially, plan not just for prevention but for response and continuity: ask "If our data was held hostage tomorrow, do we have backups and a way to operate?" [11]. Conduct tabletop exercises to simulate attacks and rehearse the IRP with the team [5]. This prepares staff to react quickly and can significantly reduce damage if an incident strike [5]. The faster an attack is identified and contained, the less the fallout. Without a plan, *"by the time you pick up the phone for help…it's probably too late."* [9].

- **Invest in Security Expertise – In-House and Outsourced**: Given lean staffing, family offices should not hesitate to bring in **outside cybersecurity** expertise. This can take multiple forms. One is hiring a full-time IT security professional or Chief Information Security Officer (even part-time/virtual) to design and oversee the program. Large family offices have begun doing so, though many smaller ones struggle with the cost justification [9]. Another approach is partnering with managed security service providers (MSSPs). Outsourced providers can monitor networks 24/7, manage firewalls and threat detection, and provide incident response on demand [14]. As PwC notes, this is especially useful if the office lacks in-house skills to continuously watch security logs and alerts [14]. In practice, most family offices use a hybrid: the Wharton GFA survey found 87% of family offices outsource some IT/cyber functions (often in addition to having some in-house staff) [10]. The key is to ensure someone, internal or external, is actively managing security

on an ongoing basis. Don't rely on a once-a-year audit; cyber threats evolve weekly. It may also be prudent to engage specialists for penetration testing and vulnerability assessments annually [9]. These "ethical hacking" tests, while costing in the tens of thousands, can reveal weak points before real attackers do. Remember, spending on expertise is an investment against far larger potential losses. One family office balked at hiring a $300K/year security lead, only to suffer a multimillion-dollar breach later [9].

- **Strengthen Technical Controls and Digital Hygiene:** Solidify the basic **cybersecurity infrastructure** protecting the family office's digital assets. Start with network defence: ensure firewalls and intrusion prevention systems are in place at all network entry points [14]. Configure these devices properly and keep firmware updated – an improperly configured firewall can be as ineffective as none at all [14]. Use encrypted Wi-Fi with strong passwords; in offices, set up a guest Wi-Fi for visitors separate from internal networks. Establish multiple network zones for different purposes to contain an outbreak or attack within a single zone. Next, enforce access controls and authentication: implement *multi-factor authentication (MFA)* on email, VPNs, and any cloud services. This single step can foil the majority of account compromise attempts. Require strong, unique passwords (consider a password manager to help staff comply). Regularly review user accounts and immediately revoke access for former employees/contractors [14]. Segment sensitive data so that even if one system is breached, an attacker can't roam freely across all information. Endpoint security is crucial too: all computers and mobile devices, if possible, should have up-to-date anti-malware protection and be set to install security patches automatically. Many breaches, especially ransomware, exploit unpatched software vulnerabilities. Something as simple as keeping Windows, macOS, and mobile OS patches current can thwart known exploits. Family principals and staff should also practice digital hygiene with their personal devices since those often connect to office data. This means routine updating of phones, tablets, and home IoT device firmware. Simple things like not updating a laptop or phone can pose a risk. Assuming someone else is taking care of these trivial tasks is dangerous" [9]. Conduct periodic security audits to ensure all these technical measures are sustained. For example, have a third party assess if cloud services (like Microsoft 365) are configured securely. One advisor points correctly out, that M365 comes with over 100 security settings, but many are *disabled by default*, so you must turn on the ones that matter [5]. In summary, cover the bases: **network defence, endpoint protection, secure configurations, and swift patching**. These are the fundamental shields that, if well-maintained, will repel a large share of opportunistic attacks and buy you time to detect more advanced ones.

- **Implement Rigorous Access and Data Management Policies:** Family offices handle extremely sensitive information. Treat it with the care a bank would. Conduct a data inventory: identify what digital assets are **"crown jewels"** (e.g. banking details, investment account credentials, legal documents, personal IDs). [10] Apply extra safeguards to those: encryption at rest, stricter access permissions, perhaps keep them off email by using secure vaults or document management systems. Limit data access on a **need-to-know basis.** Not every employee should open every file. Use rights management so that if a document is copied or emailed, it's still protected. Encourage (or mandate) use of secure communication portals for sensitive exchanges with and among family members [11]. For instance, there are family office portals that allow file-sharing and messaging in an encrypted environment, accessible only to authorized users. This reduces risky behaviour like sending bank account info or passports over personal email or WhatsApp. As Deloitte's survey suggests, many families value convenience over security in daily practice [11], so it's important to provide *user-friendly secure alternatives*. Additionally, establish clear policies around personal device use and remote work: if staff access office email on personal phones, those phones should have security controls (PINs, remote wipe enabled, etc.). Consider a modest bring-your-own-

device (BYOD) policy or use mobile device management (MDM) solutions to enforce security on any device connecting to office data. Another policy aspect is **data retention and backups**: don't keep sensitive data longer than necessary, and make sure critical data is backed up offline or in immutable storage. Regular, secure backups (with periodic testing of restore capability) are one of the best mitigations against both ransomware and accidental data loss [11]. If hit by ransomware, you can recover systems without paying criminals if robust backups exist. Finally, instill an ethos that *"any piece of information should be treated as an asset"* with an appropriate protection level [10.] This mindset will guide staff to handle data more cautiously.

- **Educate and Train Staff *and* Family Members:** The human element is paramount. Even the best technical controls can be undone by an unaware employee or an overly candid family member. Regular **cybersecurity awareness training** is a must for all family office personnel [5]. Training should cover how to recognize phishing emails, suspicious links, and social engineering attempts. It should also include **social media hygiene** (what not to post publicly) and procedures for verifying unusual requests [5]. Conduct this training at least annually, with refreshers or phishing simulation exercises more frequently. Crucially, extend the education to the family principals and their households. Often, ultra-wealthy families have multiple generations with varying tech savvy. The younger generation might overshare on Instagram, the older generation might resist new security measures. Both can introduce risk. As one EY advisor observed, a Gen-Z family member tagging their real-time location on a public Instagram from the family yacht can expose them to kidnapping or burglary risk [9]. Likewise, a patriarch (or matriarch) , who insists on using one easy password for all accounts, is a ticking time bomb. Therefore, hold periodic briefings for family members about personal cybersecurity: device updates, secure communication practices, privacy settings on social media, etc. Emphasize that their personal digital behaviour can directly impact the family office's security. Some family offices even offer cybersecurity training to domestic staff (nannies, personal assistants) who interact with the family's information or home networks. Another training aspect is practicing **incident response roles**: as mentioned, tabletop exercises help, but even simpler drills like a "phishing fire drill" (where an IT advisor sends a fake scam email to see who clicks) can be eye-opening and drive home lessons. Remember, the goal is a culture where every person is a **human firewall:** alert, informed, and following safe practices by habit. Given that **phishing is by far the top attack vector** [1], this human-centric defence is one of the highest ROI investments.

- **Manage Third-Party Risks and Vendor Security:** As discussed, third-party relationships can be conduits for attacks, so institute a robust vendor risk management program. Start by **assessing your vendors**: which service providers have access to your network or sensitive data? This can include IT/cloud providers, accounting firms, law firms, custodial banks, even building security, if they connect to your systems. For each critical vendor, vet their cybersecurity practices**.** Do they have certifications (like ISO 27001, SOC 2) or security audits? It's reasonable to ask key vendors to fill out a security questionnaire or provide a summary of controls. Next, **embed security into contracts**: require that vendors adhere to basic cybersecurity requirements and notify you promptly of any breach that could affect your data [14]. For example, if your family office data sits on a SaaS platform, the contract should mandate notification within X hours of any data breach. Many family offices now insist on such clauses and even audit rights in their support contracts [15]. Additionally, limit third-party access to only what's necessary: if a consultant needs database access for a project, ensure the account is disabled when the project ends. Use separate network segments or credentials for vendors (never share internal passwords; use guest accounts or VPN profiles that can be monitored and revoked easily). Monitor third-party activity – for instance, if your IT provider is logging in remotely, there should be logs and perhaps alerts if they log in at odd hours. **Zero**

Trust principles can be helpful: essentially, trust no one by default, whether inside or outside. Continuously verify and monitor. It's also wise to stay attuned to your vendors' security posture over time. If a key supplier has a known breach (e.g. appears in the news or on threat intel feeds), be prepared to take defensive action – maybe change passwords, or in worst cases, switch providers. In summary, treat vendors as an extension of your security boundary: **due diligence, contractual controls, and ongoing oversight** are needed to plug this often-overlooked gap.

- **Utilize Cyber Insurance and Risk Transfer (with Caution!):** Consider cyber insurance as a backstop for financial losses. Cyber insurance policies can cover incident response costs, legal fees, notification expenses, and even ransom payments in some cases. Notably, less than half of family offices currently carry cyber insurance [10], but interest is rising as attacks grow. Obtaining a policy not only provides a financial safety net but also can **drive better security practices**: insurers typically require certain security measures (the "carrot and stick" effect) [11] and will assess your controls during underwriting, which in turn gives you insight into gaps to fix. That said, insurance is not a substitute for good security. Policies have exclusions (for example, payments to sanctioned entities may be prohibited) [12], and if an office has weak controls, claims might be denied or premiums very high. Use insurance as one tool in the toolkit. (Like other forms of insurance, it should be carefully considered to understand what it covers and what it doesn't within your context as you are in many cases not protected) Ensure compliance with policy requirements (insurers might require up-to-date patching, MFA everywhere, offline backups, etc. – all of which you should be doing anyway). The process of applying can itself be instructive: the questions insurers ask can guide you to strengthen those areas. Finally, have a clear plan about how insurance would play into incident response – e.g., know when to involve the insurer, what breach coaches or vendors they provide, and what the notification obligations are. In the unfortunate event of a major incident, an insurance payout can be the difference between a financial blip and a catastrophe, but only if you've set things up correctly and met the security **"minimum standards"** that policies demand [11].

- **Cultivate a Security-First Culture and Continuous Improvement**: Cyber-risk management is not a one-off project but an ongoing process. Family offices should aim **to foster a culture of security awareness and continuous improvement**. This starts from the top: principals, boards and CEOs need to champion cybersecurity as a priority (not just lip service). When leadership asks about security in meetings, allocates budget to it, and personally follows the rules (e.g. they themselves use MFA and secure communication), it sets the tone for everyone else! Encourage open communication about cyber risks. If an employee clicks something suspicious, they should feel comfortable reporting it immediately rather than hiding it. Since technology and threats evolve rapidly, commit to **regular updates of your strategy**. For example, schedule annual reviews of cybersecurity posture: revisit risk assessments, update policies for new technologies (maybe the family started using a new fintech app or installed smart devices – those need to be accounted for). Keep an eye on emerging threats that might be relevant; for instance, deepfake fraud might prompt adding a verification step for voice instructions. Leverage insights from peers and industry groups: many family offices share anonymized threat information through private networks or at conferences. Staying plugged into such a community (or subscribing to threat intelligence services) can alert you to schemes targeting similar organizations. Additionally, consider periodic **independent audits** or penetration tests beyond your regular IT provider to get a fresh perspective [5]. Digital transformation in family offices, adopting new tech tools, should go hand-in-hand with security reviews, not lag behind. For example, if exploring blockchain or digital asset investments, ensure the custody and transaction processes are secure. If exploring AI, ensure that you have a proper

Data Loss Protection or network filters in place. Lastly, ingrain **the mindset that cybersecurity is part of the office's fiduciary duty to the family**. Just as protecting the family's financial capital is the mission, so is protecting their digital and informational capital as well. As one wealth executive aptly said, *"Cybersecurity is like insurance – a negatively skewed investment, but one you should not avoid"* [1]. In the long run, a strong security culture not only prevents incidents but also enhances trust among family members and with external partners, showing that the office is responsibly managing all facets of risk.

Conclusion

Cyber threats to family offices are **real, rising, and potentially ruinous** if left unaddressed. However, by learning from documented incidents and implementing industry best practices, family offices can dramatically improve their cyber defences. The dual nature of family offices – blending elements of private investment firms, personal enterprises, and family households – means they must adopt a **holistic cybersecurity approach**. This includes technical safeguards typical for any financial institution, *and* human-centric measures tailored to family dynamics and high-net-worth lifestyles.

For Management and board members of family offices, the path forward is clear: **treat cybersecurity as a strategic priority** integral to safeguarding the family's wealth and legacy. Allocate sufficient resources (time, budget, *expertise*) to it. The cost of proactive security is trivial compared to the cost of a major breach. Insist on accountability and metrics: for example, ask for **regular cyber risk reports**, incident attempt counts, and progress on closing vulnerabilities. Engage in scenario planning: *"What would we do if tomorrow our systems were encrypted and a $5M ransom demanded?"* If that question currently elicits silence or shrugs, it's a sign to urgently shore up your preparedness.

Encouragingly, family offices that have invested in cybersecurity show that improvements are attainable. With the right controls and training in place, some offices report fending off phishing attempts daily without incident, and turning cyber readiness into a selling point when attracting clients or talent. In an age where **ultra-wealthy families are increasingly targeted** simply because of who they are, a strong cybersecurity posture becomes as essential as legal or accounting expertise in the family office sphere. By following the strategic recommendations outlined, from governance to technical fortification to cultural change, family offices can stay one step ahead of cyber threats. In doing so, they protect not only financial assets but the very **privacy, reputation, and peace of mind** that their client families value most.

References

[1] **WealthBriefing**, "Family Offices Not Doing Enough To Thwart Cyber Attacks – Study", https://www.wealthbriefing.com/html/article.php/family-offices-not-doing-enough-to-thwart-cyber-attacks--study

[2] **Deloitte Private**, "The Family Office Cybersecurity Report 2024", family-office-cybersecurity-report-2024.pdf

[3] **Penta**, "Switzerland reports cyberattacks have doubled in the last year", https://penta.ch/insights/switzerland-reports-cyberattacks-have-doubled-in-the-last-year

[4] **Simple**., Strengthening family office cybersecurity: Key considerations for family offices looking to protect themselves against cyber threats, https://andsimple.co/insights/cybersecurity-for-family-offices

[5] **JohnReznick**, David Sun, "Cybersecurity for the family office: 3 ways to protect against threats" https://www.cohnreznick.com/insights/family-office-cybersecurity-3-ways-protect-against-threats

[6] **CNBC**, "Family offices become prime targets for cyber hacks and ransomware", https://www.cnbc.com/2024/05/21/family-offices-target-cyber-hacks-ransomware.html

[7] **Institutional Investor**, "Family Offices Are Unprepared for Cyber Threats", https://www.institutionalinvestor.com/article/2eh3jnemw9qf5mzu5gs8w/corner-office/family-offices-are-unprepared-for-cyber-threats

[8] **Presage Global**, "Combating Insider Threats in Family Offices", https://www.presageglobal.com/combating-insider-threats

[9] **Business Insider**, "The world's richest families skimp when it comes to cybersecurity, and it can cost them millions", https://www.businessinsider.com/rich-wealthy-cybersecurity-it-hack-ransomware-prevention-ey-2023-3

[10] **Ernst and Young**, Cathrine Fankhauser, "How family offices can maximize the upside of tech and minimize risk", https://www.ey.com/en_us/insights/family-enterprise/how-family-offices-can-maximize-the-upside-of-tech-and-minimize

[11] **FO Pro**, Margaret Steen, "Family Offices Are Attractive Targets for Cyber Criminals - But They Can Fight Back", https://thefopro.com/family-offices-are-attractive-targets-for-cyber-criminals-but-they-can-fight-back

[12] **Squire Patton Boggs**, "Family Office Insights - The Growing Cyberthreat to Family Offices" https://www.squirepattonboggs.com/-/media/files/insights/publications/2021/06/family-office-insights-the-growing-cyberthreat-to-family-offices/thegrowingcyberthreattofamilyoffices.pdf

[13] **J.P.Morgan**, Kevin Tompkins, Phillip Ferraro, "How to stop cybercriminals at your digital doorstep" https://www.jpmorgan.com/insights/cybersecurity/phishing/how-to-stop-cybercriminals-at-your-digital-doorstep

[14] **PWC**, Danielle Valkner, "Cyber security for family offices",

https://www.pwc.com/gx/en/services/family-business/family-office/cyber-security.html

[15] **Family Office Exchange (FOX),** "Family offices must assess 'weak links' for cyber protection", https://www.familyoffice.com/insights/family-offices-must-assess-weak-links-cyber-protection

[16] **FindLaw,** "Law Firm Sues Insurer After Ransomware Attack, $700K Lost Billings", https://www.findlaw.com/legalblogs/strategist/law-firm-sues-insurer-after-ransomware-attack-700k-lost-billings/