SAFEGUARDS

5 Practical Safeguards for Family Offices

Family offices face a unique challenge: **balancing discretion and efficiency** with the need for **robust security.** While technology plays an important role, the biggest risks often come down to **people, culture, and governance.** Here are **five safeguards** every **family office** should put in place:

1

Build a Culture of Vigilance

Cybersecurity isn't just a technical issue – it's **cultural.** Leadership must set the tone from the top. If principals and executives don't take it seriously, neither will staff.

- Make **cybersecurity awareness** part of everyday conversation.
- Provide **regular training** not just for employees, but also for family members, who may be more vulnerable to scams.
- **Encourage questioning:** it's always better to double-check than to make an expensive mistake.

2

Strengthen Governance & Workflows

Strong governance makes it harder for cybercriminals to succeed. Even the most sophisticated deepfake will fail if the right checks are in place.

- Apply the **"four eyes, not two"** principle – no major transaction should ever be authorised by a single person.
- Ensure **independent verification:** each approver must review as if they were solely responsible.
- **Reconcile all accounts regularly** against **bank records** (not just ledgers). Simple reconciliations are a powerful safeguard.
- Make **cybersecurity and reconciliation reporting** a standing item at every board meeting.

3

Verify, Don't Assume

Deepfakes succeed when people **act in haste.** Slow down and **verify requests.**

- Never trust phone numbers or details listed in an email – always use **verified contact details already saved.**
- For urgent or unusual requests, confirm **face-to-face or via secure video call.**
- Avoid relying on **one-line emails or text messages** for payment instructions.

SAFEGUARDS

5 Practical Safeguards for Family Offices (continued)

4

Get the Basics Right

Many attacks succeed not because systems are weak, but because **simple controls aren't consistently applied.**

- Use **multi-factor authentication (MFA)** everywhere — and enforce it.
- Replace passwords with **passkeys** wherever possible.
- Restrict access by **geography and role** — not everyone needs access to everything.
- **Regularly test your controls,** including backups: are they working as intended, or just assumed to be?

5

Plan for Response, Not Just Defence

Even the **best defences can be breached.** The difference between a near miss and a disaster often lies in how quickly an **organisation responds.**

- Have a **clear response plan** covering who to call, what steps to take, and how to communicate.
- **Work with trusted advisers** — legal, IT, and communications — to ensure plans are practical and rehearsed.
- Monitor for **misuse of principals' names and likenesses online,** so reputational attacks can be caught early.
- **Consider insurance** – they will have access to additional specialists that can step in during a breach.
- **Learn from incidents.** Every close call should improve your systems and culture.

CAXTON fladgate OneCollab

For a confidential conversation about your family office's cyber resilience, contact **Michael Oldham:**

BOOK YOUR CONFIDENTIAL CALL