# Comprehensive Cybersecurity for Family Offices: A Turnkey Approach

# Executive Summary

Family offices are entrusted with more than wealth. They oversee private communications, personal data, and long-term legacies—assets that cybercriminals find just as valuable as financial holdings. Cybersecurity is now their top operational concern, with 83% of single-family offices identifying cyberattacks or data breaches as their biggest risk.

That statistic is not surprising—it reflects the reality family offices face. Nearly half (43%) of family offices worldwide have been attacked in the past two years, and one in four have suffered multiple breaches.2 Those managing more than $1 billion in assets are especially at risk, with 62% reporting at least one cyberattack.

Yet, cybersecurity remains an afterthought for many family offices. One-third do not have a cyber incident response plan, and 63% lack cybersecurity insurance.4 Many rely on the default protections provided by software and hardware companies—measures designed for the average consumer, not high-net-worth families. This approach leaves dangerous gaps that attackers are ready to exploit.

Adding to this challenge, many cybersecurity providers focus only on select aspects of security or treat cybersecurity as an afterthought to physical security. Others operate on a global scale with no personalized service, making it difficult for family offices to find a true turnkey solution that aligns with their unique structure, risk profile, and privacy concerns.

This whitepaper examines the key cybersecurity challenges facing family offices and explores strategies to strengthen defenses, reduce vulnerabilities, and ensure operational resilience. By addressing both common threats and overlooked security gaps, it provides a framework for building a comprehensive, proactive cybersecurity approach.

## Why Family Offices Face Heightened Cybersecurity Risks

A cyberattack against a family office doesn't just threaten financial transactions—it can compromise private records, real estate holdings, travel plans, and even personal safety. Unlike corporate environments with dedicated security teams and enterprise-grade protections, family offices often operate with lean IT teams or inexperienced outsourced providers, creating gaps that sophisticated attackers know how to exploit.


## Why Family Offices Are at Risk

- **High Financial Exposure –** Cybercriminals see family offices as lucrative targets. 62% of family offices with AUM over $1 billion have experienced cyberattacks, compared to 38% of those with lower AUM.
- **Interconnected Personal & Business Systems –** Financial transactions, private communications, and smart home networks often share overlapping digital infrastructure, increasing attack surfaces.
- **Relying on Consumer-Grade Protections –** Many family offices assume that built-in security features from device manufacturers or software providers are sufficient. However, these mass-market solutions are not designed for high-net-worth families, who require customized, multi-layered defenses.

# Where Family Office Security Falls Short

While family offices face significant cybersecurity threats, their defenses often fail to keep pace with growing risks. These gaps leave them exposed to costly breaches, fraud, and reputational damage.

## Insufficient Risk Assessments


of family offices do not conduct security reviews of third-party vendors, even though many cyberattacks originate through compromised service providers.

## Lack of Cyber Incident Response Plans


of family offices lack a formal cyber incident response plan, leaving them unprepared to respond to ransomware, phishing, and data breaches.

## Unclear Response Protocols

Many family offices don't know who to call or what steps to take if they suspect a compromise, leading to delayed action and increased damage during an attack.

## Unclear Response Protocols

Only 8% of family offices have in-house cybersecurity personnel, and 67% have not engaged third-party cybersecurity providers.8 In addition, 63% of family offices do not require cybersecurity training for their staff, leaving them highly vulnerable to phishing, social engineering, and other human-driven attacks.

# The Most Common Cyber Threats Family Offices Face

The most significant cyber risks aren't hypothetical—they are happening now, targeting family offices with increasing sophistication.

- **Phishing and Social Engineering –** 93% of cyberattacks on family offices involve phishing.10 Attackers impersonate wealth advisors, attorneys, or even family members, tricking recipients into transferring funds or handing over login credentials.

- **Ransomware and Data Extortion –** Cybercriminals don't just lock files; they threaten to leak personal and financial information if a ransom isn't paid.

- **Insider Threats** – Whether intentional or accidental, employees, vendors, or household staff may expose critical information. Some exploit weak security controls to embezzle funds, alter financial records, or manipulate transactions without detection.

- **Unpatched Systems and Weak Access Controls** – Over 75% of family offices do not have a patch management plan for their residences, leaving networks and devices vulnerable to known exploits.11 Additionally, 50% of family offices lack a disaster recovery plan, making it difficult to respond effectively to breaches.

# Assessing Cybersecurity Readiness

Before a family office can strengthen its defenses, it must first understand where it is vulnerable. Many risks aren't obvious—they stem from outdated systems, poorly secured remote access, or third-party providers with privileged access to sensitive data.

## Key Areas to Evaluate

| | |
|---|---|
| **Device & Software Security** | Outdated hardware, missing or weak firewalls, and unpatched software create exploitable entry points for attackers. |
| **Remote Access & Network Protections** | Many family offices use unsecured remote access protocols and poorly configured port forwarding, leaving them vulnerable to unauthorized logins. Proper VPNs, firewalls, and cloud access controls must be implemented to prevent external threats |
| **Third-Party & Vendor Security** | Many breaches originate from compromised service providers. Family offices should implement strict vendor security reviews and enforce vendor security operating guidelines to minimize supply chain risks. |

Without assessing these areas, family offices leave security gaps that attackers actively exploit.

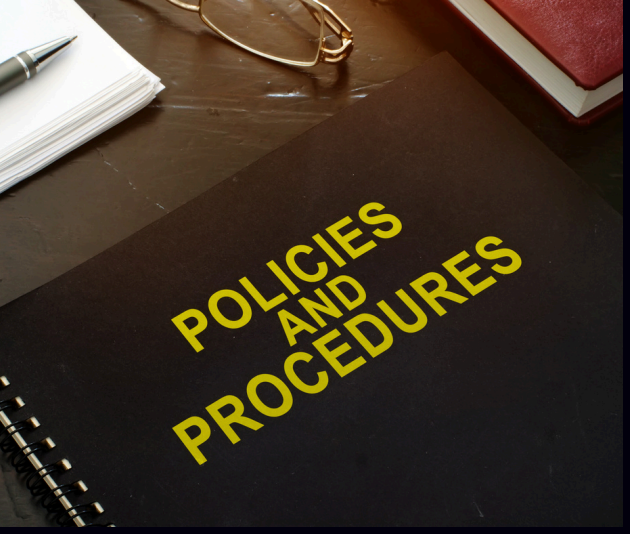
# Implementing Critical Security Measures

Once risks are identified, family offices should deploy layered cybersecurity defenses to protect financial assets, personal information, and private communications.

## Essential Security Controls for Family Offices

| | |
|---|---|
| **Adaptive Multi-Factor Authentication (MFA)** | Enhances security by using context-aware authentication, requiring passkeys, biometric verification, or risk-based challenge prompts based on user behavior, device, and location. This ensures stronger protection with minimal friction for legitimate users. |
| **Data Encryption** | Protects sensitive information both at rest and in transit, ensuring that stolen data remains unreadable. |
| **Network Segmentation** | Prevents attackers from moving freely between financial accounts, home systems, and personal devices by separating networks. |
| **AI-Powered Endpoint Protection** | Leverages advanced AI-driven threat detection, response, and real-time monitoring, backed by world-class adversary intelligence to identify and neutralize emerging cyber threats before they escalate. |
| **Routine Security Updates & Patch Management** | Ensures firewalls, routers, wireless access points, and software remain updated, closing known security gaps. |

By implementing these security layers, family offices significantly reduce the likelihood of successful attacks.




## Establishing a Cybersecurity Policy

Even the best security measures can fail if there are no defined protocols for access, data handling, and incident response. A formal cybersecurity policy ensures that family members, staff, and service providers follow established security best practices and know how to respond to a breach.

### Core Policy Components

| Network Access Control (NAC) | Passkey & Access Control Guidelines | Incident Response & Reporting |
|---|---|---|
| Establishes clear practices on which devices can access sensitive data, how remote access is managed, and enforces security requirements for all connected devices. | Implement passkeys for stronger authentication, reducing reliance on passwords. Require ecure credential storage, enforce role-based access controls, and ensure regular security updates to prevent unauthorized access. | Clearly define who to contact and what steps to take to contain threats, minimize damage, and restore security after a cyber incident. |

## Continuous Threat Monitoring & Incident Response

Cybersecurity is not a one-time effort—it requires ongoing monitoring, proactive threat hunting, and a structured response plan to contain threats before they cause damage.

### Key Security Practices

- **Automated Response to Breach Detection** - Deploys AI-driven tools that detect threats in real time and automatically isolate suspicious connections, preventing unauthorized access before a breach escalates
- **Threat Hunting –** Managed Detection and Response (MDR) shifts security from reactive to proactive, identifying reconnaissance activity and potential attackers surveilling your systems. By detecting attack vectors early, family offices can disrupt threats before they take hold.
- **Incident Response Planning and Testing–** Establishes a clear, step-by-step framework for handling breaches, ransomware attacks, and fraud attempts. Regular security audits test the plan's effectiveness through simulated cyberattacks and penetration testing to ensure readiness.


of family offices lack an incident response plan. Without a structured breach containment strategy, recovery becomes slower and costlier. A proactive approach ensures threats are identified, contained, and neutralized before they can cause lasting damage.

## Where Traditional Approaches Fall Short

Despite increasing cyber risks, many family offices continue to rely on inadequate security strategies, often without realizing the extent of their exposure. The most common missteps include:

| Assuming Consumer-Grade Security Is Enough | Using Fragmented Security Services | Lacking a Unified IT and Cybersecurity Approach |
|---|---|---|
| Built-in protections from hardware manufacturers and software vendors are designed for general consumers, not for high-net-worth families managing multi-million-dollar assets and sensitive personal data. | Some providers only monitor specific devices or accounts, leaving home networks, personal communications, and financial systems exposed. Without a holistic view of potential threats, vulnerabilities remain unaddressed. | Many firms treat cybersecurity as an afterthought rather than integrating it into IT infrastructure management. This disjointed approach creates security gaps that attackers can exploit. |

These oversights give cybercriminals an advantage, allowing them to target under-protected family offices that mistakenly believe they are secure.

# The Case for a Turnkey Cybersecurity Approach

Rather than relying on default protections or ad-hoc solutions, family offices need a fully managed, proactive cybersecurity strategy—one that integrates threat detection, IT security, and rapid response into a single, seamless defense system.

## What a Turnkey Approach Provides

Rather than relying on default protections or ad-hoc solutions, family offices need a fully managed, proactive cybersecurity strategy—one that integrates threat detection, IT security, and rapid response into a single, seamless defense system.

- **Comprehensive Network & IT Security** – Family offices need more than just cybersecurity; they require full IT oversight to secure home-office networks, financial systems, and personal devices under one managed framework.
- **Real-Time Threat Detection & Incident Response –** Security Operations Centers (SOC) and Security Information and Event Management (SIEM) systems provide 24/7 monitoring, ensuring that suspicious activity is detected before it leads to a breach.
- **Advanced Threat Hunting –** Cybercriminals constantly evolve their tactics. Rather than waiting for an attack, threat hunting actively scans networks for signs of intrusion, stopping attacks before they escalate.
- **Encrypted Communications & Credential Protection –** Financial transactions, private emails, and sensitive data require end-to-end encryption, Adaptive (MFA), and dark web monitoring to prevent unauthorized access.
- **Dedicated Cybersecurity Experts –** Unlike IT consultants who offer generic security add-ons, a dedicated cybersecurity team specializes in the unique threats facing high-net-worth families, providing hands-on support and customized risk assessments.
- **Rapid Breach Response & Recovery –** Cyberattacks unfold in minutes. A turnkey approach ensures immediate containment, forensic analysis, and system restoration to minimize financial and reputational damage.

## Conclusion: A Smarter Approach to Family Office Cybersecurity

Family offices oversee financial and personal assets that require strong, adaptable security. Yet, many rely on default protections or fragmented IT solutions, leaving them exposed to sophisticated cyber threats. A proactive, integrated approach—one that combines real-time threat detection, encrypted communications, and continuous monitoring—is essential for long-term protection.

Decypher Technologies provides discreet, tailored cybersecurity solutions designed specifically for family offices. With expertise in both cybersecurity, and IT, broadband, and cellular infrastructure, Decypher ensures seamless, fully managed protection across every aspect of your digital environment.

To learn how to secure your family office,
contact Decypher Technologies today.

decypher™
TECHNOLOGIES