

WRITTEN BY CASEY SELL

WHEN CYBER RISK BECOMES PHYSICAL RISK

For high-net-worth families and family offices, security is no longer defined solely by gates, guards, alarm systems, and access controls. Today, some of the most significant exposures originate in the digital world: a compromised password, a spoofed email, a social media post, a fraudulent invoice, or even a short voice recording. Cyber and physical risks are no longer separate concerns. Increasingly, they are connected in ways that can create financial, operational, reputational, and even personal safety consequences.

An attacker may begin with online research, stolen credentials, or a compromised email account and then use that access to commit fraud, impersonate a trusted individual, or create a real-world safety threat. What starts as a cyber event can quickly become something much larger.

One of the most common examples is **invoice fraud**. A family office may unknowingly pay a fraudulent invoice that appears to come from a legitimate vendor. According to Medius' 2024 Financial Professional Census, invoice fraud costs the average U.S. company more than \$1 million annually, with average losses of approximately \$133,000 per incident.¹ These are not isolated events. They have become increasingly sophisticated, often arriving with fabricated approval chains, professional-looking PDFs, forged tax documents, and email threads designed to appear completely legitimate.

Impersonation fraud has evolved just as rapidly.

Staff members or family members may receive a phone call that sounds exactly like a principal, executive, or trusted relative, only to discover later that the voice was generated using artificial intelligence. These deepfakes use AI to replicate a person's voice, appearance, facial expressions, and mannerisms with remarkable realism, making it increasingly difficult to distinguish authentic communications from fraudulent ones. In a widely reported 2019 case, criminals used AI-generated audio to imitate a parent company executive's voice, accent, and cadence, convincing a subsidiary CEO to transfer approximately \$243,000.²



By 2024, these attacks had expanded well beyond audio. A finance employee in Hong Kong joined what appeared to be a routine video conference with several senior colleagues. **The participants were later discovered to be deepfakes; AI-generated video replicas designed to convincingly mimic a person's appearance, voice, facial expressions, and mannerisms in real time. Before the deception was uncovered, more than \$25 million had been transferred through fifteen separate transactions.**³ The speed with which these attacks have evolved demonstrates how quickly traditional trust-based controls can be bypassed when technology is used to convincingly impersonate trusted individuals.

The concern is no longer theoretical. According to a 2025 survey cited by WealthManagement.com, **83% of family office advisors reported specific concern about deepfake and impersonation campaigns** targeting principals and high-net-worth clients.⁴ Separately, **Deloitte's Family Office Cybersecurity Report found that 43% of family offices experienced a cyberattack during the previous 12 to 24 months**, and 18% of those affected reported suffering a financial loss.⁵

Family offices are particularly attractive targets because they possess a unique concentration of financial, personal, and operational information. When that information is compromised, the consequences extend beyond identity theft or financial fraud. **Home addresses, travel schedules, school routines, household staffing information, and asset locations can all become valuable intelligence for criminals seeking to conduct surveillance, extortion, social engineering, or other forms of physical targeting.**

For families who own yachts, cyber and physical risks can converge around a single asset. **A modern yacht is not merely a luxury vessel; it is also a sophisticated technology platform that relies on navigation, communications, monitoring, and location systems.** If those systems are compromised or disrupted, the consequences may extend beyond data loss. Location information could expose a vessel's movements, while interference with onboard systems could create broader operational or security concerns.

From an insurance perspective, these exposures are particularly complex because a single event can trigger multiple forms of coverage. A personal cyber policy may respond to the initial intrusion, fraud event, or extortion demand. If the incident escalates into piracy, ransom demands, physical damage, or liability exposures, other coverages such as Hull & Machinery, Protection & Indemnity (P&I), or Kidnap & Ransom policies may also come into play. Even families with multiple policies in place can face significant gaps if those coverages have not been evaluated together.



The challenge is no longer determining whether cyber risk is an information technology issue or a physical security issue. **It is both.**

As a result, family offices should routinely evaluate several key questions:

- How are wire instructions and payment requests independently verified?
- What personal information about family members, residences, travel schedules, and assets is publicly available?
- How would a deepfake or impersonation attempt be identified and escalated?
- Which insurance policies would respond if a cyber incident resulted in a financial loss, extortion demand, or physical security event?
- Where do those policies overlap, and where might coverage gaps exist?

Cybersecurity, physical security, and insurance can no longer be evaluated independently. The most resilient family offices recognize that today's threats often begin digitally before manifesting in financial loss, reputational harm, or physical risk. **Understanding how these exposures connect, and how insurance coverage responds when they do, is increasingly becoming a core component of effective risk management.**

-
1. Medius, 2024 Financial Professional Census, as reported in CFO.com, **"Invoice Fraud Costs Average Company More Than \$1M Per Year."**
 2. Jesse Damiani, Forbes, September 3, 2019, **"A Voice Deepfake Was Used To Scam A CEO Out Of \$243,000"** (originally reported by The Wall Street Journal).
 3. CNN, February 4, 2024, **"Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'"** (incident later identified as involving Arup and confirmed by Hong Kong Police).
 4. Omega Systems 2025 Financial Services Cyber Resilience Survey, as reported by WealthManagement.com, **"The Growing Cybersecurity Threat to Family Offices."**
 5. Deloitte Private, **The Family Office Cybersecurity Report 2024**. Deloitte reported that **43% of family offices experienced a cyberattack during the prior 12 to 24 months, and 18% of those affected reported a financial loss.**



CASEY SELL

Private Client Family Office Director

casey_sell@ajg.com | (757) 434 8724

The information contained herein is offered as insurance industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer financial, tax, legal or client-specific insurance or risk management advice. General insurance descriptions contained herein do not include complete insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis.

Gallagher publications may contain links to non-Gallagher websites that are created and controlled by other organizations. We claim no responsibility for the content of any linked website, or any link contained therein. The inclusion of any link does not imply endorsement by Gallagher, as we have no responsibility for information referenced in material owned and controlled by other parties. Gallagher strongly encourages you to review any separate terms of use and privacy policies governing use of these third-party websites and resources.