BOSTON PRIVATE

WEALTH ▫ TRUST ▫ PRIVATE BANKING

Demystifying Risk Management for FAMILY OFFICES

EXAMINING TRENDS, FRAMEWORKS, AND BEST PRACTICES IN AN EVER-EVOLVING RISK ENVIRONMENT.

By Edward V. Marshall

TABLE OF CONTENTS

INTRODUCTION

When principals establish a family office, typically, the goal is to create a centralized management system to more efficiently and effectively manage assets, decision-making, and services under one roof. By their very nature, family offices are discreet, often maintaining reduced public profiles to anonymize activities of the office and the principals they serve. Despite these efforts, malicious actors have become aware of what family offices are, where they are, and how they operate. As a result, they have become an increasingly attractive target for criminals and other nefarious characters. While family offices manage the wealth and assets that are often associated with small- and medium-sized companies, they often do not employ the necessary risk management policies, technologies, and personnel.

In this paper, we explore the increased risks that family offices face, why family offices are at risk, and provide recommendations to improve risk management.

WHAT ARE THE RISKS FAMILY OFFICES FACE?

The Internet is full of stories to give family office principals and executives pause, including:

- Cyber breaches resulting in wire fraud that are connected to national state conflicts or nation states collaborating with criminals;
- Investment losses due to major problems and liabilities not being uncovered in due diligence;
- Cyber-enabled physical threats stemming from increasingly interconnected devices (smart homes, yachts, vehicles, etc.);
- Complex identity theft schemes against Fortune 500 CEOs;
- Fraud perpetuated by trusted "insiders" that goes undetected for years;
- Bugged boardrooms which are uncovered through technical countermeasure sweeps;
- Kidnapping and ransom of the children and spouses of principals while traveling abroad; and
- Exploitation of social media accounts to stalk family members and/or steal compromising pictures or information.

Risks to wealthy families are nothing new. John D. Rockefeller, and other magnates of his era, used family offices to oversee their vast fortunes. However, Rockefeller's family office never had to deal with cyber ransomware attacks or privacy breaches stemming from the social media accounts of his children.

The evolving landscape of how family office security and risk systems can be breached has made the task so much harder. Executives continue to struggle to find effective ways to deal with these multi-faceted threats (physical, financial, health, cyber, and privacy-related).

While risks to family offices may not be new, the services that family offices are expected to deliver continue to increase in complexity. Family offices are responsible for a wide array of advisory and service needs for their families (Figure 1).

FIGURE 1: THE SIX KEY SERVICE AREAS FOR FAMILY OFFICES

ADMINISTRATION, ACCOUNTING, AND TAX	INVESTMENT STRATEGY AND MANAGEMENT	ESTATE MANAGEMENT AND COMPLEX ASSETS	PHILANTHROPY AND IMPACT INVESTING	GOVERNANCE AND FAMILY SERVICES	RISK AND THREAT MANAGEMENT

While they differ in the breadth, complexity, and timing of their needs, all family offices generally are tasked with risk and threat management for principals in some form or another (Figure 2).

These tasks include background checks of employees, due diligence of potential deals, complex legal advice, personal and business insurance coverage, physical security, privacy, and cybersecurity.

Unfortunately, most family office staff are not prepared for the level of risk exposure that the activities of the family creates because they:

- Do not have a background as security professionals;
- Do not possess assigned personnel/outside advisors to manage the family office threat profile;
- Do not have access to or awareness of expert resources to address myriad of threats;
- Do not properly train employees (or for that matter family members and external advisors); and/or
- Do not consider the risks of performing services that, while accommodative to the needs of the family, sacrifice security.

Criminals are not going to go away, but family offices can adopt best practices, making them a harder and less attractive target.

WHY ARE FAMILY OFFICES AT RISK?

Family offices are often staffed by sophisticated and highly-experienced personnel who are not naive to the kind of threats faced by wealthy families. With the anecdotal examples of what not to do and the abundance of expert service providers in the field, why do family offices continue to struggle with risk management?

FIGURE 2: RISK AND THREAT MANAGEMENT SERVICES FOR FAMILY OFFICES

RISK AND THREAT MANAGEMENT

- Insurance
- Legal Services
- Personnel Evaluation and Monitoring
- Privacy and Reputation Management
- Physical Security
- Investigative Advisory
- Cybersecurity
- Medical Advisory and Advocacy
- International Travel

The three primary flaws that cause ineffective risk and threat management strategies for family offices revolve around the mindsets of principals and executives, organizational designs of family offices, and governance. For family offices, these flaws (Figure 3) generate the following underlying issues that inhibit proper risk management:

1. Underestimation and overlooking of threats
2. Frustration and perplexity concerning effective protective measures
3. Reactionary mindset

WHAT CAN FAMILY OFFICES DO TODAY?

The following are recommendations that family offices can use to overcome these three underlying factors and start improving their risk and threat management postures. These focus on creating better risk and threat awareness among family members, family office staff, and risk management service providers. Also, included are suggestions for how better risk management data can lead to an even stronger defense against family office threats.

"Nation States and sophisticated actors are increasingly focusing on Family Offices and high-net-worth individuals as targets of financial, data and identity theft. We have seen a growing trend of targeted attacks on this sector due to many factors, including the disconnect between the cyber security industry and the product needs of family offices as well as the poor digital hygiene associated with growing family offices. Sound cyber security for a family office does not necessarily mean large expenses for personnel and tools. Effective solutions can often be found in basic awareness training and sound architecture."

- Mike Janke, Co-Founder of Data Tribe

FIGURE 3

UNDERESTIMATION AND OVER-LOOKING OF THREATS	FRUSTRATION AND PERPLEXITY OVER EFFECTIVE PROTECTIVE MEASURES	REACTIONARY MINDSET
FAMILY OFFICE PERSPECTIVE: *"We're under the radar."*	**FAMILY OFFICE PERSPECTIVE:** *"Don't know where to start."*	**FAMILY OFFICE PERSPECTIVE:** *"We're putting out other more immediate fires."*
CAUSES: • Lack of reliable benchmark data of threats against family offices. • Misperceiving risks because of a lack of awareness. • Self-diagnosis of risk and threat exposures resulting in gaps.	**CAUSES:** • Scarcity of vendors with tailored approaches for family offices. • Lack of context and experience with risk management. • Absence of frameworks to understand the risk management vendor landscape.	**CAUSES:** • Insufficient strategic planning and informal governance mechanisms across the family office enterprise. • Operational prioritization of convenience over security.

BACKGROUND AND FRAMEWORKS

As discussed earlier, family offices are challenged with a growing number of risk and threat management issues. They make attractive targets for criminals because of the magnitude of wealth they manage and the different types of attacks (cyber, physical, financial, privacy, hybrid, etc.) that can exploit family office structures and activities.

I) UNDERESTIMATION AND OVERLOOKING OF THREATS.

The belief by many families that "privacy equals security" has been undermined by the advent of the Digital Age. David Dezso, CEO of Banyan Risk Group, highlights the scope of the challenge: "Within 15 minutes and with $15, an attacker can know more about a person or entity than most expect. Things like where you work, your home address, your vehicles purchased and plenty more. It is getting harder to hide in the modern digital era and most family offices are left underprepared and vulnerable."

Many family offices continue to conflate a focus on privacy as a shield against threats by believing that living "under the radar" is adequate protection. With that mindset, they risk failing to uncover potential threats through self-diagnosis.

The misperception that only large corporations and governments face the majority of sophisticated attacks makes the family office susceptible to miscalculation as to the need for sophisticated countermeasures. In reality, the majority of cybersecurity attacks are conducted against small- and medium-sized companies with family offices falling into that category.

In this section, we explore three underlying causes as to why family offices underestimate and overlook threats: 1) lack of reliable benchmark data of threats against family offices, 2) misperceptions of risks because of lack of awareness, and 3) improper self-diagnosis of risk and threat exposures.

"In an effort to resolve these issues, family offices have increasingly turned to external resources for assistance. However, the service offerings on the market today to help them manage these risks are most often broken down into traditional single areas of expertise focused on solving only one problem set. This results in services being offered in "silos" such as physical security and executive protection, event security, IT and cyber-security and other singular disciplines. Even those purporting to offer advanced Security Operations Centers ("SOC"), usually only focus on digital/cyber or physical security monitoring. The result, is family offices are being provided fragmented and incomplete advice."

- Karl V. Hopkins, Partner and Global Chief Security Officer, Dentons

LACK OF RELIABLE DATA, ANALYSIS, AND BENCHMARKS OF THREATS AGAINST FAMILY OFFICES.

Despite the professionalization and maturation of the family office industry, there is a dearth of tailored and actionable data, analysis, and benchmarks on risk management for family offices. The lack of relevant data makes it difficult for family office executives to make compelling cases to their principals about the need to reevaluate current practices and to identify what basket of security solutions the family office needs. Campden's 2019 Global Family Office Report sheds some needed light on the risk management problems that family offices face, and also demonstrates how there is much more research needed to better understand the issues in this space.

Campden's report highlights the increasing attention that family offices place on risk management. In a global survey of family offices, 20% of family offices reported that they suffered a cyberattack. The actual number of cyberattacks against family offices is likely higher given resource constraints for detection and the general reluctance for family offices to admit that they have been defrauded or attacked. Despite the increasing threat environment, there is some good news regarding sentiment and awareness. Campden's findings also show that in a ranking of top governance priorities for their family office, respondents placed "Risk Management" at the top. The increased focus on planning for and knowing how to properly mitigate risks is a sign that family offices are starting to appreciate that they have a problem that requires increased attention and action.

However, there is much room for improvement on the data front. Knowing that you have a problem versus knowing the scope, scale and appropriate countermeasures, are two different matters. Yet, despite how far the family office industry has come, there is a lack of well-sourced data. Family offices lack good data on a variety of factors including:

- What parts of the family office should be monitored and how?
- How much should the family office spend on risk management and security?
- What vendors are best suited to work with family offices?
- What risks are coming and how can family offices protect themselves against them?
- What are similar family offices doing for risk management, and how are they implementing those procedures?

MISPERCEIVING RISKS BECAUSE OF A LACK OF AWARENESS.

In general, family office executives have a mixed sense for the potential risks and threats they face given their professional experiences. Executives who run these offices come from various backgrounds, but traditionally have experience as accountants, attorneys, or financial services professionals. In addition, many professionals migrate (partially or fully) from working for a family's operating business to running their personal affairs. These professionals—however skilled at handling the investments, finances, or operations of a complicated business—do not have the same experience in risk management as do cybersecurity or due diligence professionals.

In addition, while many family office executives have experience working at large and complex multinational companies with sophisticated risk and threat management systems, they often miss key risk factors applicable to family offices. Despite the fact

"The risks to family offices are no different than to financial institutions, law firms or information technology providers – they contain a treasure trove of sensitive and potentially lucrative information and malicious actors want it. Believing you are off the radar because there are larger companies to target or that there are not a lot of news reports of family offices being defrauded or hacked, is a mistake."

– Chad Sweet, CEO, The Chertoff Group

"In a new world fraught with risks of bad guys doing bad things – stealing profits, IP, reputations and wreaking havoc – family offices and their crown jewels are now being targeted. Bank robber Willie Sutton was famously asked why he robbed banks and his reply was, "Because that's where the money is." A trend we are seeing is top security and risk management talent are now being aggressively courted by family offices to play defense against today's proverbial Wille Sutton's."

– Jeremy King, Benchmark Executive Search

that these companies face many of the same risks as wealthy families, the operational idiosyncrasies of a family office, coupled with the relative lack of investment in risk management systems, professionals and training, makes family offices more susceptible to successful attacks. In these cases, executives from large multinational firms may not have the context necessary to see looming risks. As a result, they may fail to properly anticipate exposures and build systems to mitigate or prevent them from happening.

SELF-DIAGNOSIS OF RISK AND THREAT EXPOSURES.

As discussed previously, family office principals and executives sometimes mistakenly conflate their personal focus on privacy as a shield against risks and threats. Getting and staying "off the grid" in an increasingly interconnected world will be more challenging in the future. With a slight modification to an old adage*, "just because you're not paranoid, doesn't mean someone isn't out to get you." Unfortunately, the notion that only large corporations and governments are the targets of criminals, is widespread among family offices and this only makes them more susceptible.

II) FRUSTRATION AND PERPLEXITY OVER EFFECTIVE PROTECTION MEASURES.

SCARCITY OF RISK VENDORS WITH COMPREHENSIVE AND RELEVANT APPROACHES TO THE FAMILY OFFICE INDUSTRY.

Companies that provide risk and threat services are certainly not in short supply. The security services industry (physical and investigative services) generates approximately $40 billion in revenue.[1] Growing at a fast pace, IT security consulting was estimated to be a $16 billion industry and expected to grow at nearly 7% in 2019.[2] The number of family offices with a net worth greater than $250 million are also on the rise.[3] The nearly 18,000 family offices around the world–growing at nearly 8% each year–represents nearly $16 trillion in wealth, according to data from Wealth X.

KNOWING WHERE TO GO FOR ANSWERS TO RISK MANAGEMENT QUESTIONS.

How does the family office staff select its risk management service providers? Family office executives often struggle with finding the right person to call to solve a risk-related problem. Too often, an executive will lean on a person within their personal network (former law enforcement officer, intelligence professional, or a friend in the military). Rarely do executives have relevant contacts with appropriate security experts with enterprise-level experience and a history of working with family offices.

Once a family office executive exhausts his or her personal network, they invariably search for public information about family offices and risk advice or solution providers. However, given the dearth of publicly available information, and the limited marketing to family offices by security and risk management firms, this approach may lead to less robust and effective solutions than are needed. Executives may be missing out on related, unexpected threats not picked up when they solve a particular risk problem. As Wesley Bull, CEO of Sentinel Resource Group notes, "Today's security threat environment is highly dynamic, evolving and multi-dimensional. As such, residual entanglement risks can be overlooked when leaders overly focus on

*The common phrase states that 'just because you are paranoid, doesn't mean someone isn't out to get you.

[1] Security Services Industry in the US - Market Research Report. Site: https://www.ibisworld.com/united-states/market-research-reports/security-services-industry/

[2] IT Security Consulting Industry in the US - Market Research Report. Site: https://www.ibisworld.com/industry-trends/specialized-market-research-reports/technology/computer-services/it-security-consulting.html

[3] World Ultra Wealth Report 2019. Source: Wealth-X

FIGURE 4 **THE FAMILY OFFICE RISK VENDOR LANDSCAPE; RISK AND THREAT CONSEQUENCES**

- PROPERTY DAMAGE
- DISCLOSURE OF SENSTIVE INFORMATION
- HEALTH ISSUES OR DEATH
- BUSINESS DISRUPTION
- IDENTITY THEFT
- KIDNAPPING OR STALKING
- WORKPLACE VIOLENCE
- REGULATORY PENALTIES OR LAWSUITS
- THEFT OF INTELLECTUAL PROPERTY
- LOSS ON INVESTMENTS
- FINANCIAL OR LIQUIDITY ISSUES
- TECH OR OPERATIONAL FAILURE
- CRISES OR DAMAGE TO REPUTATION
- BURGLARY OR ROBBERY
- FRAUD AND EMBEZZLEMENT
- ASSAULT

LACK OF BENCHMARKS ▪ LACK OF RISK AWARENESS ▪ SELF-DIAGNOSIS OF THREATS
VENDOR SERVICES MISALIGNMENT ▪ LACK OF STRATEGIC PLANNING FOR RISK MANAGEMENT
PRIORITIZATION OF CONVENIENCE OVER SECURITY

RISK SERVICES CATEGORIZED BY SOURCE OF THREAT TO A FAMILY OFFICE

INTERNAL SOURCES

- Background checks on employees and business/personal associates
- Insider threat program - family and employees
- Personal security awareness training
- Workplace threat management and training
- Continuity of operation
- Common operating picture

BLEND

- Investment and general business due diligence
- Regular threat assessments
- Psychological profiling
- Acute medical emergencies
- Chronic medical conditions
- Reputation management
- Internet of things
- Crisis management

EXTERNAL SOURCES

- Protective details
- Residential, estate, and commercial facility security
- Threat intelligence
- Kidnapping and terrorism threat management
- Private aviation and maritime security
- Collectibles and high value item security and logistical support
- Technical security countermeasures
- 24/7 watch centers
- Natural disasters

a specific silo of security risk, rather than recognizing these varied threat vectors are part of an overall ecosystem of risks to the principal and/or family office."

A strategy better suited for this new threat environment integrates working with advisors who not only have extensive risk management experience, but also have contextual experience of working with many family offices.

ABSENCE OF FRAMEWORKS TO UNDERSTAND THE RISK MANAGEMENT VENDOR LANDSCAPE.

Figure 4 above is a framework that can be used as family offices and security firms develop comprehensive strategies. Effective security requires understanding both outcomes and preventative measures so that families can properly defend themselves and service providers can provide applicable solutions. The barrier between service providers and family offices is a two-way street. Family offices are not armed with the expertise, contacts, or context to find the ideal service providers for their specific issues.

Conversely, most risk management service providers lack a nuanced understanding of how best to interact with family offices and do not have relationships with these private families. As a result, these service providers often struggle to match their unique experience and expertise to the needs of this client segment. Both parties walk away with suboptimal outcomes.

III) REACTION TO ISSUES AS THEY EMERGE. INSUFFICIENT STRATEGIC PLANNING AND INFORMAL GOVERNANCE MECHANISMS ACROSS THE FAMILY OFFICE ENTERPRISE.

While the principals who form family offices are often sophisticated entrepreneurs and business owners, very few family offices develop and deploy robust strategic plans and management processes. A primary driving factor behind this behavior, is that principals initially form their family offices around their specific and often immediate needs. Coupled with the lean monetary and personnel resources that family offices are often afforded, they don't have the luxury of long-term planning exercises when more pressing operational issues are at hand.

This creates a paradox in that family office strategic planning is viewed as necessary and logical to outsiders, while strategic planning takes less precedence and makes the least amount of sense to family office insiders. That said, the lack of strategic planning processes creates tangible risks for family offices, especially in terms of preparing for "shocks" to the family office ecosystem.

There are numerous examples of family fortune losses due to the lack of family structure and interconnectedness, family member power struggles, and untested and ill-equipped heirs. Family offices tend to operate with a flat management structure and, in general, lack a detailed operational "playbook". So, why is this important when considering strategic planning of risk management?

The culture, ethos, habits, and idiosyncrasies of how family offices approach strategic planning are critical to understand when considering risk management. Because of their very nature, many family offices will maintain a reactionary mindset tackling problems as they arise. While this mindset might be tolerable for certain aspects of a family office, it is often behind some of the serious problems seen when family office risk management programs are poorly designed and operated. Losses due to financial fraud, intrusions of privacy, personal security, etc., are magnified when the family office's risk management response efforts are constantly having to play catch up.

Family offices can combat this issue by developing a strategic risk plan in which they take action by:

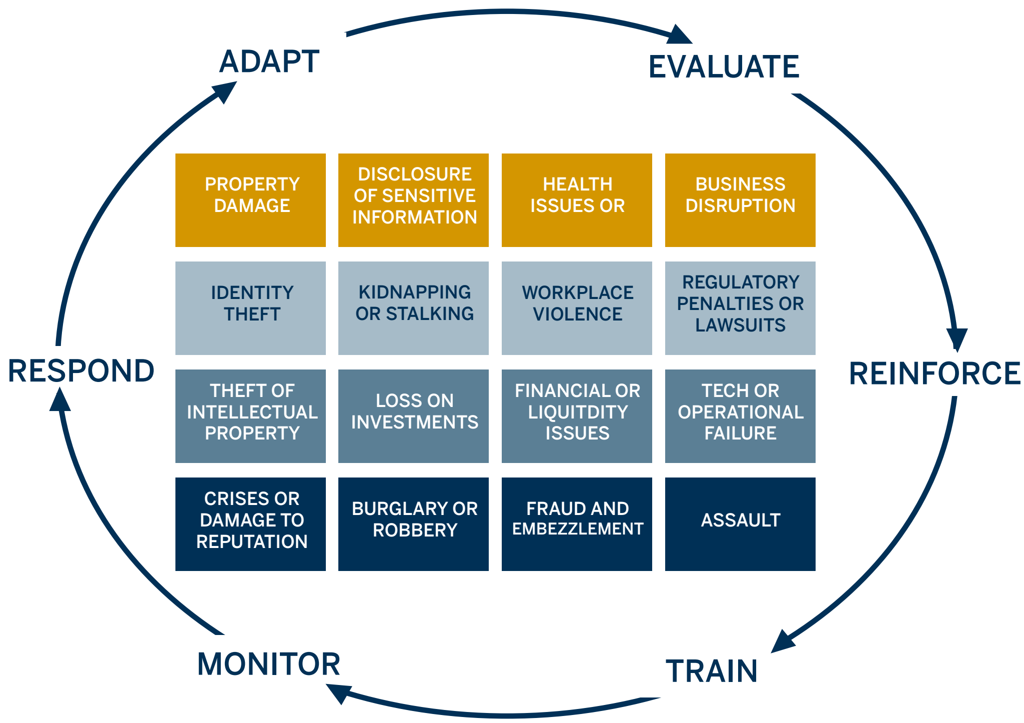
- Developing a rudimentary reaction plan around all of the risk consequences described in Figure 4;
- Hiring security consultants to train and test preparation levels of family office staff and principals;
- Conducting annual reviews of family office risk exposures to identify gaps and update plans accordingly; and
- Developing a network of family offices to share best practices and vendor recommendations.

As they become more professional, hire staff with broader management experience, and as the operational

"Whatever strategy or tactics a family office employs to assess their overall risk, a strong reaction is to have professional threat mitigation guidance from experts who have broad knowledge and are able to provide support, guidance and solutions tailored to the family office's unique problems and circumstances. Family offices should not rely on off-the-shelf solutions or tools that are designed to fit general problems, due diligence inquiries, or point solution software platforms to provide effective physical or cyber security."

- Lon Augustenborg, CEO, Novus Intelligence

FIGURE 5: FAMILY OFFICE ENTERPRISE RISK MANAGEMENT



complexities of running a family enterprise increase, family offices are developing and employing more traditional forms of corporate strategy. While this trend is still in its early days, the most successful heads of family offices will develop, manage, and measure progress as part of a strategic risk management process.

OPERATIONAL PRIORITIZATION OF CONVENIENCE OVER SECURITY.

The very nature of family offices creates another critical factor in suboptimal risk management practice. The culture of family offices requires them to often focus on efficiency, responsiveness, and speed of task completion to the detriment of risk and threat management. These expectations can cause unnecessary, preventable, and unexpected exposures to risks that could be mitigated with proper policies and procedures.

Fraudsters are increasingly aware of this issue and have exploited it for their gain. A common example of this problem occurs with wire transfers, when principals are unavailable to confirm the transaction for legitimate reasons (foreign travel, death in the family, etc.). In such schemes, criminals create an urgency for the transfer of funds that seems legitimate because it fits the pattern of the principals (e.g. purchasing art/collectibles). Usually these fraudulent requests will come via email or text message.

The family office, then, fails to follow established procedures for confirming transfer requests via phone calls to principals, because they are focusing on efficiency and trying not to “bother” the principal. The end result, is a transfer of funds to a malicious party which is nearly impossible to recover.

WHAT FAMILY OFFICES CAN DO TO PROTECT AGAINST RISKS

In order to adequately protect a family office against risks and threats, should families in-source a large team made up of former CIA case officers, FBI Hostage Rescue Team members, or Navy SEAL DEVGRU Special Operators? There answer is, clearly, “no.” However, navigating the divide between the two specialized worlds can be challenging. Partnering with experts from these types of backgrounds is just one component of establishing a secure family office enterprise. The key to success of any risk management plan is the development of an “all risk” approach that takes the entire family enterprise into account. This approach requires integrating proactive and reactive policies and measures across the different outcomes of risk. Figure 5 provides an approach that family offices can use to develop and deploy a comprehensive security management program.

To jump start their strategic risk management planning, family offices should begin with a baseline assessment. Risk and security consultants can provide this through an annual evaluation that incorporates the risk outcomes discussed in this paper. These evaluations should incorporate critical elements such as staff/principal interviews, evaluations to identify gaps, and surveys of risks at residences and workplaces.

Most importantly, family offices should insist on evaluations that go beyond “desktop due diligence” which rely heavily on open-source/public information. Family offices should insist on evaluations that combine publicly-available and non-public information because criminals will try to find non-public information in order to enhance their attacks. Risks are always evolving; therefore, regular assessments coupled with proper training and procedures will help families maintain a strong risk management plan.

There are many competent and qualified security vendors who can provide certain aspects of a holistic enterprise risk management solution. Evaluation of providers can be challenging, but armed with the resources described earlier in this paper, family offices can better understand and resource their risk management strategies.

Awareness of the risks that family offices face can also benefit service providers as they approach this customer segment. As family offices evolve, the needs across the six key service areas (Figure 1) are likely to change. Advisors that a family relied on when they sold their company 10 years or a generation ago, might need to be augmented to adapt to today's needs. Risk management is subject to those same changing dynamics, even more so when it involves technology advancements. As part of their risk management program, families should regularly examine their vendors to see if service upgrades or additional help is warranted.

Here are a list of questions that families can use to build or enhance their current enterprise risk management program:

- When was the last time we conducted a complete evaluation of all the internal/external risks and threats that our family office and family enterprise face?
- What is our annual budget for the family office and how much of that budget do we have allocated to risk management?
- How important is attorney-client privilege as part of our risk and threat management strategy?
- What do we do and who do we call when faced with a crisis such as a cybersecurity breach, if our child is exposed to social media bullying, or if family confidential information is being leaked to the media?
- What types of risk and threat issues has the family or family office faced in the past?
- What risks are a persistent "back of the mind" concern that are not adequately mitigated?
- What succession plans do we have in place should principals become incapacitated or die?
- What are our disaster recovery plans for physical, financial, and digital assets?
- What are our insurable exposures? When did we last have them evaluated and updated? How are they being mitigated?

WHAT THE FAMILY OFFICE INDUSTRY NEEDS

The key to success in working with family offices is to understand their motivations and be cognizant of their concerns in all matters. The executives and principals of family offices are sophisticated and well-accomplished professionals in their individual disciplines. However, as described in this paper, family offices still tend to underestimate and overlook threats, struggle with effective protective measures, and maintain a reactionary mindset.

The culture and nature of family offices puts them at a distinct disadvantage when it comes to effective risk management. Criminals are always adapting new methods and technologies to commit fraud against family offices. The saying that, "Generals always fight the last war," is fitting vis-à-vis family offices and their risk management strategies. Just as military strategies can mistakenly rely on old methods to fight evolving threats, family offices, too, are susceptible to underestimating and failing to prepare for the risks they face. Moreover, criminals will use asymmetric tactics against family offices, often leveraging inexpensive methods to penetrate a family office's defenses.

However, there are ways that family offices and service providers can band together to benefit everyone.

The family office industry needs better data and benchmarks that both advisors and family offices can use. A census on family office risk management–incorporating the elements described in this paper–would provide principals, executives, and service providers with invaluable insights to operate more effectively and securely across the enterprise.

Coupled with participating in this risk survey, family offices would benefit from a tailored risk management conference where they could:

- Receive a detailed briefing on a family office risk survey;
- Learn about the emerging threats and best practices of risk management from other family offices and top-tier advisors;
- Meet service providers with relevant family office experience, as well as emerging experts and technology;
- Enjoy peer-to-peer networking with family office executives and principals to discuss risk management and other potential collaboration issues (direct deals);
- Get regular updates and actionable information on critical and emerging family office risk management issues before and after the conference.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

— Sun Tzu

Sun Tzu's quote on knowing yourself and your enemy applies to this risk survey and associated conference. Armed with this knowledge and networking connections, family offices will be better prepared to face today's risk management issues and those that could present problems in the future.

Boston Private has partnered with leaders in the family office industry to create such a comprehensive family office survey, conference, and related materials. We believe that this pioneering work will benefit family offices and their advisors for years to come.

Learn more at bostonprivate.com/familyoffice.

ABOUT THE AUTHOR:

Edward V. Marshall is a Managing Director responsible for leading business development and account management of UHNW and family office relationships for the firm's Private Banking, Wealth & Trust business. He also helps lead the Family Office practice and spearheads strategic initiatives within commercial bank at Boston Private. He is a noted author, consultant, and subject matter expert on family offices, and advises family offices around the world. Mr. Marshall is based in New York City.

Mr. Marshall joined Boston Private from Citi Private Bank, where he was a Director in the Global Family Office Group and led business development and program management for the North American Family Office team. He also advised clients on the critical aspects of running a family office, including organizational design, governance, and privacy and reputation management. He has published numerous whitepapers on these topics. Prior to joining Citi Private Bank, Mr. Marshall was a member of the UHNW and Family Office practice at Credit Suisse and managed client relationships as a Relationship Manager. He joined Credit Suisse from Booz Allen Hamilton where he was a member of their Organization and Strategy Practice. Mr. Marshall began his career in the public sector working for the federal government in the United States and abroad.

He earned his MBA from New York University's Leonard N. Stern School of Business and a B.S. in human biology from Michigan State University. He is also a guest lecturer on wealth management at New York University's Stern School of Business.

00832_20200214