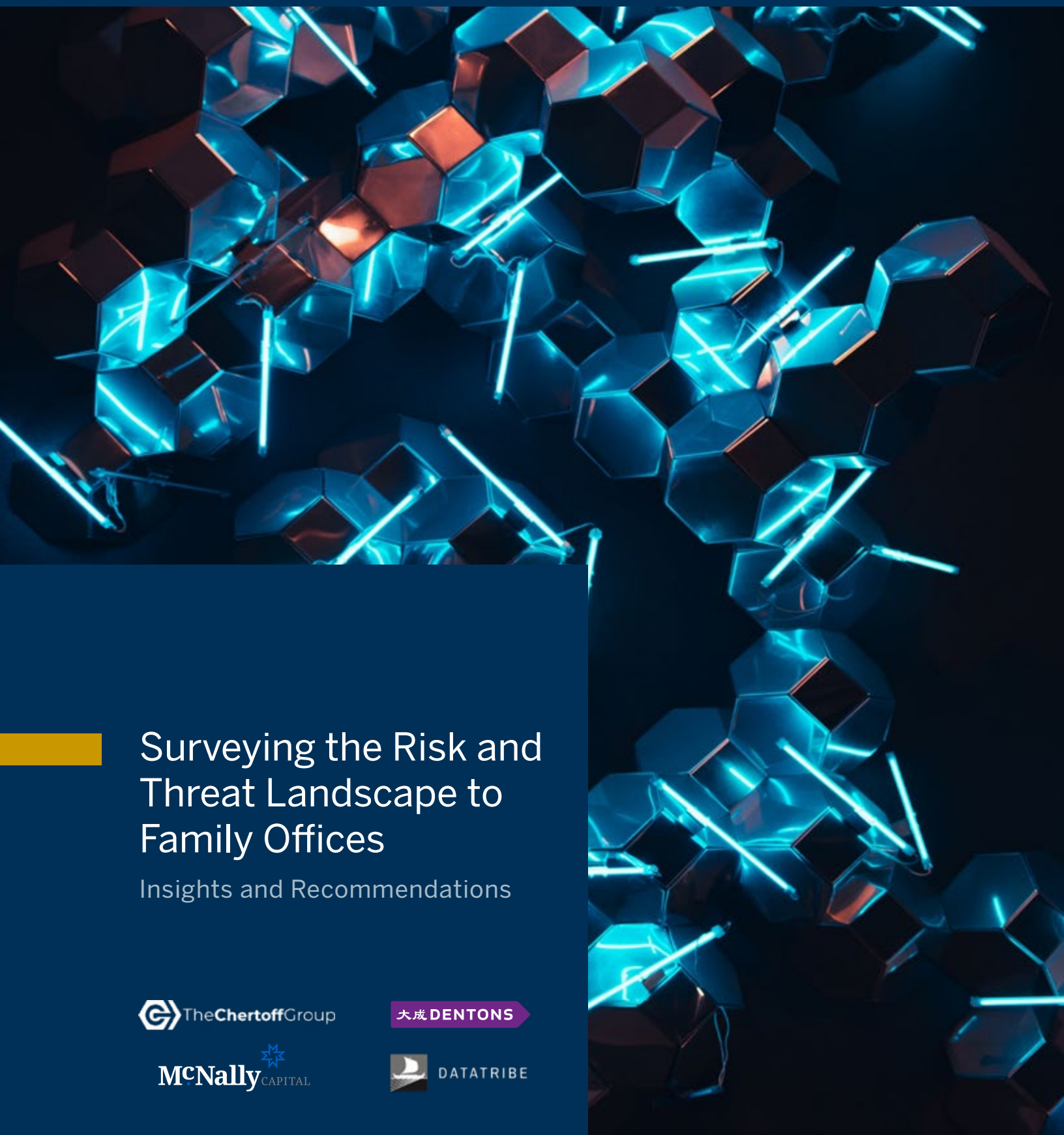
BOSTON PRIVATE

WEALTH ▫ TRUST ▫ PRIVATE BANKING



Surveying the Risk and Threat Landscape to Family Offices

Insights and Recommendations

TheChertoffGroup

大成 DENTONS

McNally CAPITAL

DATATRIBE

Contents

3 **Foreword**

4 **Executive Summary**

6 **Introduction**

8 **Risk and Threat Management Overhaul Needed**

9 A Culture of Underestimating Risks and a Need to Change Family Office Mindsets

11 Over 25% of Family Offices Have Been Hacked... Now What?

13 Misconceptions Over the Threat of Cyberattacks

14 The COVID-19 Challenge

15 Family Offices and Cybersecurity

18 Smaller Family Offices by Asset Size Underestimate Cyberattacks

20 Security Incidents at Family Offices

21 **Misalignment of Needs and Services**

22 A Need for a Better Coordinated Set of Risk Management Services

22 International Travel and Health Advisory Services Are Critical Risk Services but Infrequently Implemented by Family Offices

23 How Family Offices Are Tackling Cybersecurity

24 Family Offices Fail to Carry Out Regular Background Checks on Staff

25 Tail Risk is a Key Focus for Family Offices

25 Reputational Risk is Neglected by Most Family Offices

26 Family Offices Need to Look to Outside Risk and Threat Expertise

27 Family Offices Use Training to Counter Risks – But Is It Enough?

28 **Family Offices and Their Use of External Vendors**

29 Balancing the Need for Outsourcing: Family Offices Tend to Insource Financial Risk Personnel and Outsource Cybersecurity-Related Risk Services

30 Family Offices Are Increasingly Training Staff on Potential Risks but More Rarely Have Plans or Stress Test Those Reaction Plans

31 Effectively Using External Vendors for Risk Management Can be a Challenge for Family Offices

32 Selecting Risk Management Vendors

33 Plugging the Knowledge Gap

34 **Practical Tips and Recommendations**

36 **Background of the Survey**

38 **Our Survey Partners**

Foreword

If 2020 has taught us anything, it is the importance of planning and preparing for the unexpected.

Family offices, like all of us, are adapting to our new, largely-remote environment — though it presents new risks they must address and contain.

Family offices are no strangers to risks and threats. However, quite often they struggle to identify effective ways to deal with these matters. Part of the struggle stems from a lack of data and research that can help family members and staff make more effective decisions.

As a result, our team developed this risk and threat survey to provide critical decision-making data that could be leveraged by both principals and executives in the family office.

While it is true that family offices are uniquely designed around the needs of a principal, there are best practices that families can integrate to increase the effectiveness of outcomes and operations. This survey aims to provide some of those best practices related to risk and threat management.

We want to thank our survey partners who were instrumental in this project: The Chertoff Group, Dentons, McNally Capital, and Datatribe. Our partners lent access to their extensive networks of family offices and provided their global expert insights to support the key learnings we present in this report.

We would also like to thank a member of our own team, Edward V. Marshall, for his work on this report. Edward took the survey from concept to development, applying his family office, risk and threat management expertise throughout the project.

We hope that you will find the information in this report useful as we navigate the current pandemic environment and prepare for a post-COVID-19 world and beyond.

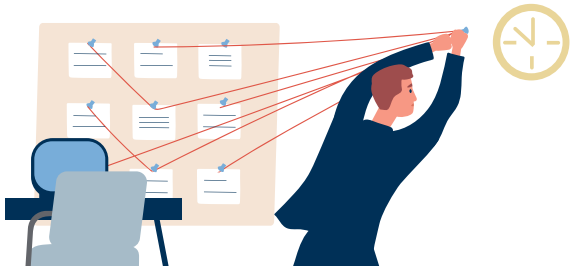
Anthony DeChellis
CEO
Boston Private

Bill Woodson
Head of Wealth Advisory and Family Office Services
Boston Private

Executive Summary

An online survey conducted by Boston Private with over 200 family office executives at single and multi-family offices, primarily in the US, has uncovered some worrying approaches to the risks family offices face, particularly cyber risk, family-related risk, investment risk and employment-related/insider risks.

1



POOR RISK MANAGEMENT MINDSETS

A change in mindset is needed at many family offices, which either underestimate threat levels (47%) or are complacent about risks (41%). Limited staff, as well as an emphasis on cost and convenience, are other obstacles to better risk management.

2

PREVALENCE OF CYBER ATTACKS ON FAMILY OFFICES

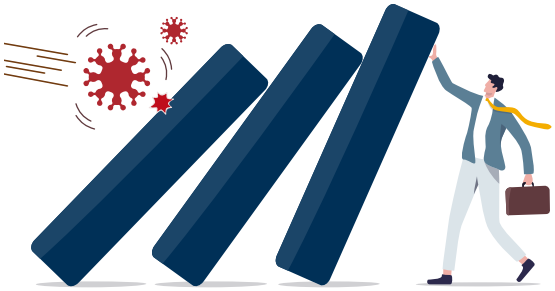
Over a quarter (26%) of family offices have suffered a cyberattack. In almost two-thirds of these cases, it happened within the last 12 months.

3

UNDERESTIMATING CYBER RISKS

Smaller and newer family offices underestimate both the likelihood (15% compared to 25% at larger family offices) and potential impact of cyberattacks (38% expect a major or catastrophic impact from a cyberattack compared to 52% at larger family offices). Older and larger family offices are more likely to have implemented cybersecurity measures (60% versus 31% for newer family offices).

4



LACK OF COVID-19 READINESS

Almost three-in-ten family offices (29%) did not have a business continuity plan in place before the COVID-19 pandemic. And over a quarter (27%) said implementing secure remote working protocols is one of their top risk management challenges.

5

NEED FOR INCREASED TRAINING AND STRESS TESTING

While over half (58%) of family offices have trained employees and family members on risks, only around a quarter (28%) have conducted stress tests or scenario analysis to back up training and planning.

6

NEED FOR BETTER INSIDER THREAT INTEL AND PROCEDURES

Eighty one percent do not conduct periodic background checks on all personnel, with 68% only doing this when staff are first hired.

7

FINDING GOOD VENDORS IS A CHALLENGE

For over a third (35%) of family offices finding a good external risk and threat management vendor is a major challenge, along with a lack of tailored approaches for family offices (35%) among external vendors.

8

POTENTIAL RISK VULNERABILITIES CAUSED BY THIRD-PARTY VENDORS

Over a quarter (28%) of family offices have never carried out a review of the risks and threats from using a third-party vendor.

9

A FOCUS ON DOWNSIDE INVESTMENT RISK

Mitigating tail risk is the most common primary focus for family offices (36%) when considering investment risk.

10

HEALTH AND TRAVEL RISKS ARE NEGLECTED

International travel and health advisory risk and threat management services are neglected by a large majority of family offices. Only 16% use medical advisory services, despite the disruption from significant health issues and the increasing sophistication of medical advisory and risk management tools.

11

NEED FOR A STRONG PEER NETWORK OF FAMILY OFFICES CENTERED AROUND RISK

Over a quarter of family offices have developed a network of family offices to share best practices and vendor recommendations, while almost 60% want to see more conferences to help do this.

Introduction

Family offices sometimes fall through the cracks of being big enough to be specifically targeted, but not having in place the strong risk management measures typical of bigger organizations, hence leaving them very vulnerable.

– Kevin Hulbert,
Dentons LLP

The risk and threat landscape for family offices continues to evolve and present new challenges. COVID-19 created new risk issues for families to consider and manage, but a pandemic is only one dimension of the increasingly complex threats that family offices face.

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 risk and threat management 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).

Moreover, the attitudes of many principals and family office executives around risk opens this group up to specialized problems. Vendors and families alike have seen this manifest itself in: 1) an underestimation and overlooking of threats; 2) frustration and perplexity concerning effective protective measures; and 3) a reactionary mindset at family offices or constantly putting out operational fires.

The figure on the next page provides a view of the multitude of risks and threats that family offices face and a list of services that vendors have available to protect and mitigate those problems. The figure also illustrates the common barriers that prevent both family offices and vendors from working effectively today, specifically around:

- Lack of relevant risk and threat benchmarks for family offices;
- Lack of risk awareness by family offices;
- Self-diagnosis of risks and threats by family offices;
- Misalignment of vendor services and a lack of relevant experience in working with family offices;
- Failure to implement strategic planning around risk and;
- General complacency or prioritization of convenience over security in a family office environment.

THE FAMILY OFFICE RISK VENDOR LANDSCAPE: RISK AND THREAT CONSEQUENCES

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

To study these issues with an aim to shed light on some of the underlying causes of these problems, we conducted a research project to better understand the family office risk landscape. We asked over 200 family office insiders to give us their thoughts on risk and threat matters they face every day. The results were illuminating and answered many questions and provided some unexpected insights into the risk management characteristics and behaviors of family offices. These findings open new areas to evaluate and present opportunities for families and vendors to address risk more effectively.

Risk and Threat Management Overhaul Needed

A Culture of Underestimating Risks and a Need to Change Family Office Mindsets

Family offices face a range of challenges, from an uncertain investment climate, to the repercussions of the global COVID-19 pandemic, to the operational challenges of maintaining privacy and managing assets securely in a digital world. While most family offices, manned by experienced and capable professionals, may feel able to cope with the investment issues they face, risk and threat management is becoming a tougher nut to crack. While their relatively small size can bring advantages, such as speed and flexibility, the inherently limited budget at many family offices can make risk management more challenging due to a potential lack of resources and specialized expertise.

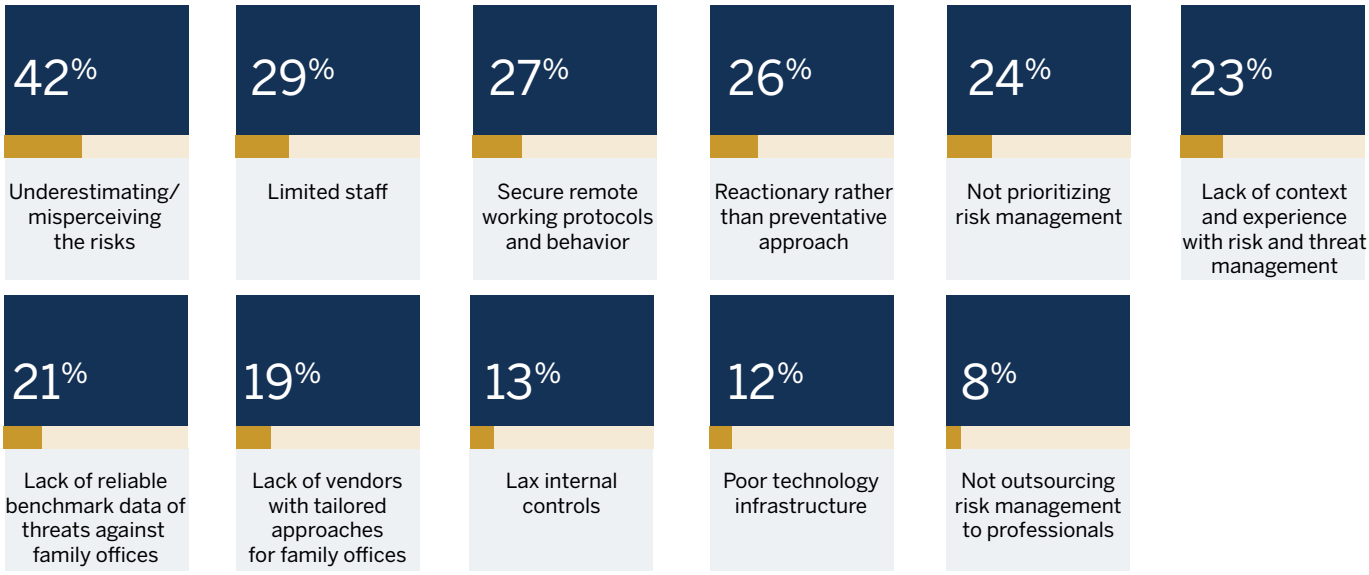
Furthermore, if family offices lack the internal expertise, controls, and technology infrastructure to defend against the wide-ranging hazards they face, then the threat of these risks could be multiplied by poor attitudes towards risk management, characterized by a mindset of complacency and underestimating risk.

The survey findings clearly show how a dangerous combination of limited resources and poor attitudes could expose family offices in terms of risk management. For instance, 42% of respondents put underestimating or misperceiving the risks as one of their top risk management challenges. If risks are being underestimated, this helps explain the finding that 41% of respondents state that complacency is one of the main obstacles in implementing risk management measures in their family office.

Other findings provide more evidence that family offices are in danger of falling short on risk management, due to deficiencies in their mindset and culture, as well as a lack of suitable resources. So while 29% of family offices say having limited staff is a top risk management challenge, this is compounded by around a quarter (26%) of family offices having a reactionary, rather than preventative approach as one of their top risk management challenges, along with 24% agreeing that not prioritizing risk management is a significant challenge.

Family Offices Face Various Risk Management Challenges

What are the top risk management challenges for your family office?



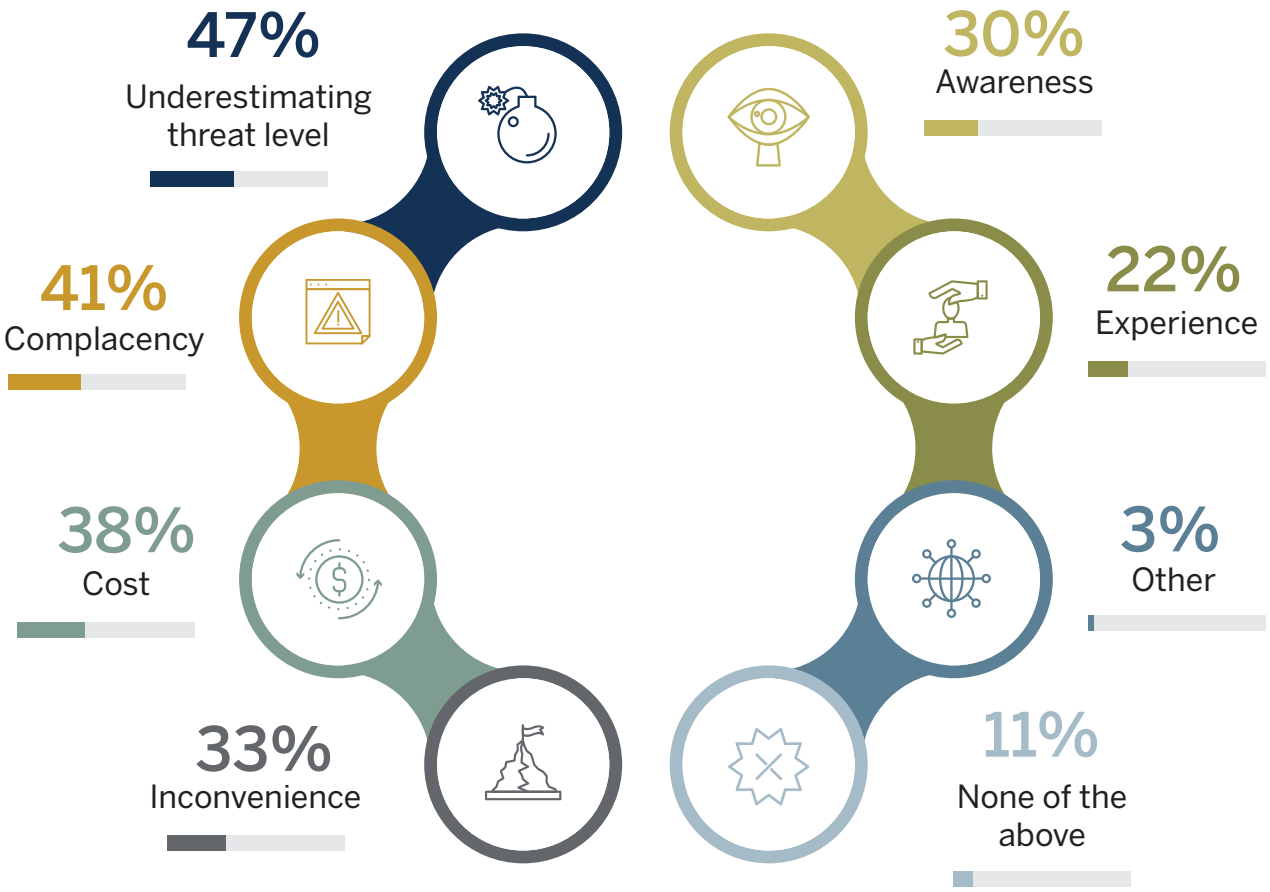
% Yes, Multiple answers allowed

Allied to the challenges of remote working and risk management, nearly a quarter (23%) of family offices put a lack of context and experience with risk and threat management as a top risk management challenge. A smaller number (13%) see lax internal controls as a top risk management challenge, while 12% cite poor technology infrastructure and just under one-in-ten (8%) cite not outsourcing risk management to professionals as risk management challenges for family offices.

Two other risk management challenges are finding reliable benchmark data on the threats to family offices and also vendors with tailored approaches to family offices. Around one-in-five family offices give these two issues as top risk management challenges for them. Again, these challenges add to the worrying picture of a lax and complacent approach to risk management, and a lack of staff and other resources that are needed.

Underestimating Threats and Complacency Are Obstacles to Risk Management At Family Offices

What are the main obstacles to implementation of risk management measures in your family office?



% Yes, Multiple answers allowed

As well as needing to improve their mindset towards risk management, family offices also face cost and inconvenience, among other obstacles to risk management. Nearly four-in-ten (38%) family offices cite cost as a main obstacle and a third (33%) see inconvenience as an obstacle. Awareness (30%) and experience (22%) can also be obstacles to implementing risk management measures at family offices. These findings further show that family offices need to address both cultural issues and also find the resources needed to ensure that their risk management systems are capable of dealing with the mix of threats they face.

Of note is that on the one hand so many family offices are open about their security shortcomings… acknowledging that they routinely underestimate/ misperceive the threats… but on the other hand, 54% of family offices believe they are prepared for the risks next year. This disconnect shows the importance of working with outside experts to help see the forest through the trees and to protect against complex risks.

– Chad Sweet, The Chertoff Group

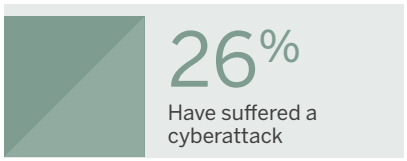
Over 25% of Family Offices Have Been Hacked… Now What?

Just over a quarter (26%) of family offices have suffered a cyberattack in the past and nearly a fifth (17%) say this has happened within the last 12 months. These results show that cyberattacks are a very real threat for family offices.

Cyberattacks against family offices

Has your family office suffered a cyberattack in the last 12 months?

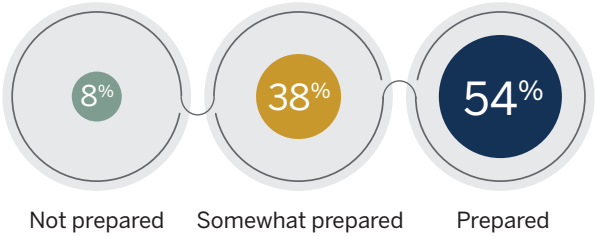
Has your family office ever suffered a cyberattack?



Over half (54%) of family offices say that they are prepared for risk to their organization in the coming year, while 38% are somewhat prepared. However, this finding is at odds with other results, such as the fact that 47% of respondents say underestimating the threat level is obstructing the implementation of risk management in their family office, or that 41% say that complacency is an obstacle to the implementation of risk management measures at their family office. These findings strongly suggest that many family offices are overestimating their risk management capabilities, especially when taken with other findings on the risk management challenges faced by family offices.

Family Offices on Their Risk Management Abilities

How prepared are you in dealing with risks to your organization in the coming year?

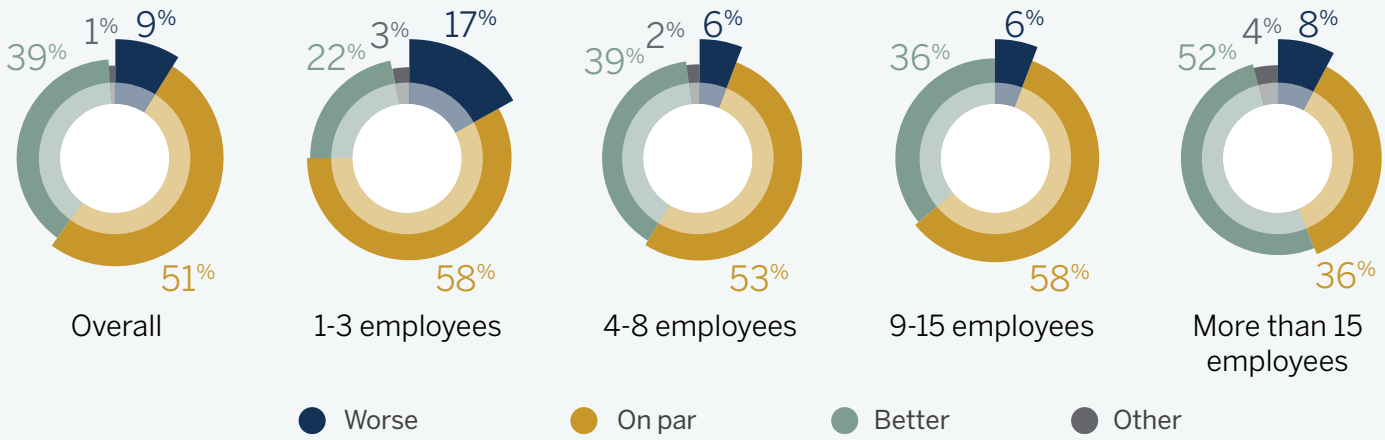


The risks of overestimating risk management programs by family offices are also shown by the finding that 39% of respondents think that their family office risk management program is better than their peers, while 51% see it as being on a par with their peers and only 9% see it as worse than their peers. These results are consistent with the finding that as many as 41% of family offices say that complacency is an obstacle to risk management at family offices. In any event, the mismatch between these findings and results elsewhere suggest that a comprehensive review of risk management could be very timely, given the fact that cyberattacks are becoming more common and remote working is increasingly the norm, due to COVID-19.

When comparing themselves to their peers, smaller family offices with less staff are less likely to rate their risk management program as better than their peers. Only 22% of family offices with three or fewer staff do this, compared to 52% for family offices with more than 15 staff, 36% for those with nine to 15 staff, and 39% for those with four to eight staff. Here, smaller family offices are likely to be less sophisticated in terms of using risk management programs and also be aware of this shortcoming.

Larger Family Offices See their Risk Management Programs as Better

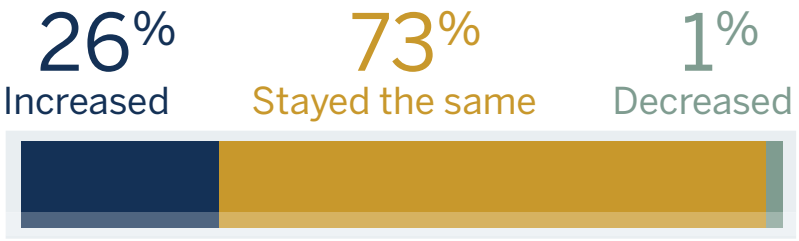
Relative to your peers, how would you rate your family office risk management program?



Almost three-quarters (73%) of family offices say their overall risk budget in their family office has stayed the same in the last year. One in four (26%) say it has increased and only 1% say it has decreased.

Most Risk Budgets Unchanged in the Last Year

How has the overall risk budget in your family office changed in the last year?



Misconceptions Over the Threat of Cyberattacks

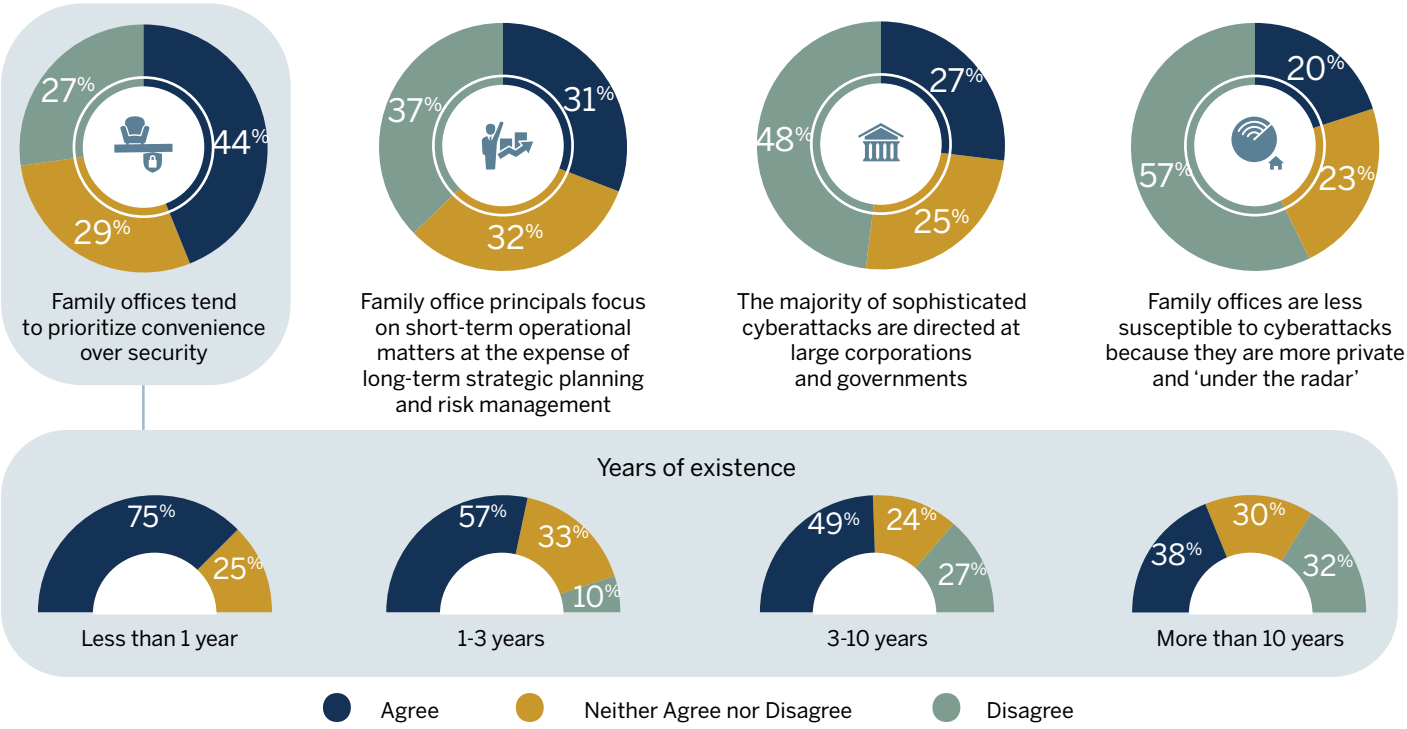
The survey finds that family offices could be vulnerable to cyberattacks as a result of misconceptions about the nature of cybercrime and a focus on short-term convenience over longer term planning and risk management. This further backs up the findings on a poor mindset and resource constraints which may hamper effective risk management.

44% of family office respondents agree that family offices tend to prioritize convenience over security, while 31% agree that family office principals focus on short-term operational matters at the expense of long-term strategic planning and risk management (and 32% are neutral on this). These findings add weight to the view that risk management is less of a priority and focus for family offices than it should be.

At the same time, many respondents see cyberattacks as less of a threat to family offices, compared to larger and more prominent institutions. Over a quarter (27%) of family office respondents agree that the majority of sophisticated cyberattacks are directed at large corporations and governments, while exactly a quarter are neutral on this. And a fifth of respondents believe that family offices are less susceptible to cyberattacks because they are 'under the radar' and another 23% are neutral on this.

Taken together, this indicates that there are family offices with a weak grasp on security and risk management, and who also believe that cybercriminals are less likely to target family offices, which could, in the circumstances, be a dangerous belief to hold.

Many Family Offices Focus on Convenience and the Short-Term



One interesting finding here is that newer family offices are more likely to agree that family offices tend to prioritize convenience over security. Over half (57%) of family offices in existence for up to three years agreed or strongly agreed, with this, compared to 49% in existence for three to 10 years and 38% in existence for more than 10 years. Here, it is likely that older family offices have learned through experience that security is more important than convenience, a lesson which younger family offices are likely to learn with the passing of time.

> *Family offices face the challenge that there is little or no ROI on proving a negative from what-if scenarios. For every dollar spent in other parts of a FO or organization, security many times is overlooked because it cannot be measured until a problem occurs. At that point, it's too late. Remediation and incident response could cost orders of magnitude higher compared to being proactive and being ready with an effective defensive risk and threat management game.*
>
> – Jeremy King, Benchmark

The COVID-19 Challenge

The COVID-19 pandemic is likely to have stress-tested the business contingency planning, among other aspects of risk management, at family offices. Many family office staff will have had to work remotely during lockdown, which brings additional challenges to the security of IT networks and data.

The risk management challenge of the pandemic could have proved a major test at nearly a quarter (23%) of family offices, where a lack of context and experience with risk and threat management is seen as a top risk management challenge. In addition, a smaller number of family offices give lax internal controls (13%) as a top risk management challenge, while 12% cite poor technology infrastructure as a risk management challenge for family offices. These findings show how some family offices lack some of the basic requirements for proper risk management in normal circumstances, let alone the stresses of remote working during a pandemic.

Remote Access Is a Challenge for Family Offices

Knowing what you know now about the COVID-19 pandemic, what is one thing you would have done differently at your family office?

"Worked on developing a reliable system of conducting meetings in a non-face to face capacity."

"Better contingency planning for lockdowns and restrictions on travel."

"Would have been better prepared to have all staff working from home, with access to network."

"Have a more formal work from home plan with cybersecurity and operational risk addressed."

As shown, while most (71%) of family offices had a business continuity plan in place before December 2019, this still leaves 29% who did not. And business continuity plans can vary in quality and their robustness in the face of a pandemic. Similarly, over half (57%) of family offices said they were prepared for the pandemic, but almost a third (32%) classed themselves as "somewhat prepared" and a further 11% said that they were not prepared.

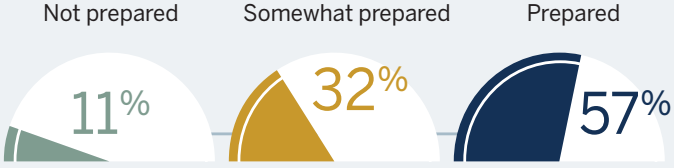
Asked what they would have done differently, had they known what they know now about the COVID-19 pandemic, the answers show that family offices, like many other businesses, were left scrambling to catch up. It is likely many contingency plans did not consider the prolonged restrictions on business travel or lockdowns imposed in the pandemic, nor the need for reliable and secure ways of conducting virtual meetings. And some family offices would have wanted to have put in place more formal plans for working from home, with full consideration of cybersecurity and operational risks.

Finding: 29% of families failed to have a business continuity plan before the pandemic

Did your family office have a business continuity plan in place before December 2019?

Preparedness for COVID-19

How well was your family office prepared for the COVID-19 pandemic?



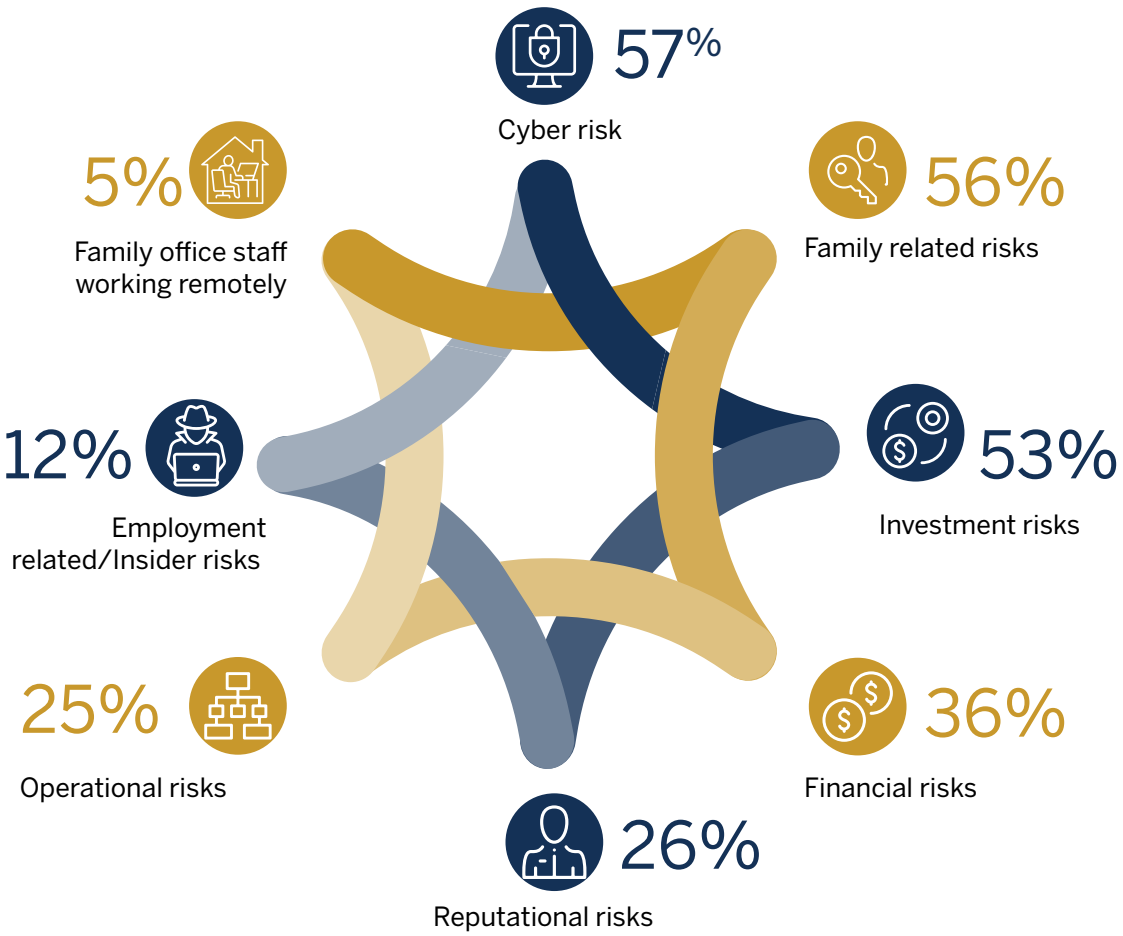
Family offices continue to underestimate the risks associated with remote working, insider threats, and supply chain risks from vendors

While some do not feel that family offices are a major target for cyberattacks due to their relatively small size and low profile, it is clear that cyber risk is regarded as a big risk by family offices. In fact, 57% see cyber risk as one of the biggest risks faced by family offices, ahead of family related risks (56%) and investment risks (53%).

Looking at the other results here, it is surprising that the risks arising from family office staff working remotely are placed so low; only 5% see this is one of the biggest risks that family offices face. Given that 2020 has seen the COVID-19 pandemic lead to a huge increase in remote working, all organizations, including family offices, need to be vigilant about the increased dangers of cyberattacks and other cyber risks. This is because a natural disaster, such as a pandemic, can create opportunities for cybercriminals and other malicious actors. With more staff working remotely for extended periods, staff are more likely to be on less secure home wifi for an internet connection, or using personal or shared devices for work purposes, so IT security standards are likely to have fallen during the pandemic. Even if family offices can extend their IT perimeter from office premises to cover remote working sites, then there are other cyber risks to consider.

Family Offices See Cyber Risk as a Leading Risk

What in your opinion, are the biggest risks family offices face?



% Yes, Multiple answers allowed

For example, family offices may be less likely to update software during the pandemic, for fear of upsetting IT systems which are already stretched. But software updates often tackle security faults and a failure to update software regularly can open the door to hackers and other bad actors.

According to reports in trade publications, institutional investors, such as asset managers, pension funds, or endowments and foundations, are seeing an increase in cyberattacks[1]. This trend is unlikely to exclude family offices. Indeed, if their risk management systems are lacking and their mindset is poor, they could be seen as low-hanging fruit by those with criminal intentions. The data held by financial institutions is an attractive prize for hackers and other cybercriminals, or they may seek to trick investment organizations into transferring them money electronically. Other cyber threats include ransomware, where criminals seize control of an organization's software systems and demand payment, or obtaining confidential data which can be used for illegal purposes or sold on the dark web to other criminals.

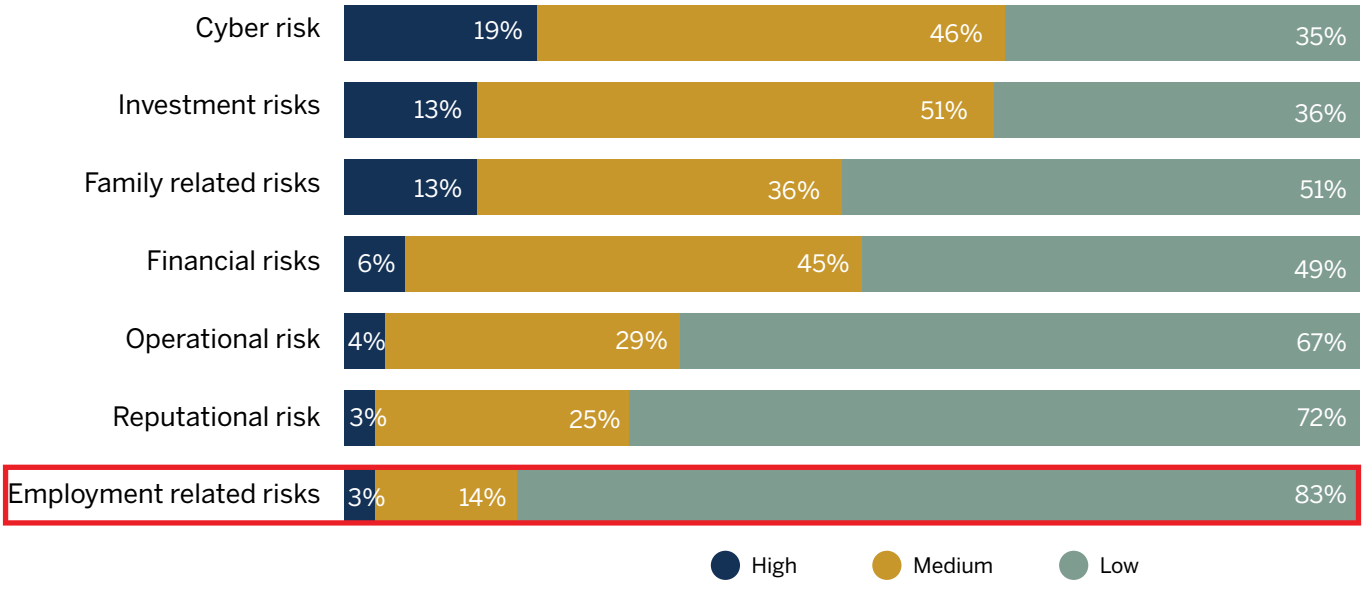
While some still have an outdated image of cybercriminals as consisting of nerdy teenage hackers, the potential prizes on offer are drawing organized crime gangs, who now realize that cyber crime carries a lower risk of detection and higher illegal rewards than some of their traditional activities. In a globalized world, family offices are at risk to cybercriminals from around the world, as long as they have a laptop, an internet connection and sufficiently developed IT skills.

One of the reasons that family offices see cyber risk as first among a host of risks is its likelihood of happening as a threat in the next 12 months. Nearly a fifth (19%) of family offices believe the chances of cyber risk materializing in the next year are high, with a further 46% putting this as a medium risk.

Investment risks are seen as having a high likelihood in the next year by 13% of family offices, with 51% putting them as medium risk. Family related risks have a lower overall likelihood, with 13% putting them as high and 36% as medium. These results show that respondents are aware of the rising incidence of cyber risk in general and are concerned that it could affect their family office in the next 12 months.

Family Offices See Cyber Risk as a Likely Threat in the Next Year

What is the likelihood of these risks materializing at your family office over the next 12 months?



[1] "Cyber Attack Hits Prominent Hedge Fund, Endowment, and Foundation", *Institutional Investor*, October 24, 2019.

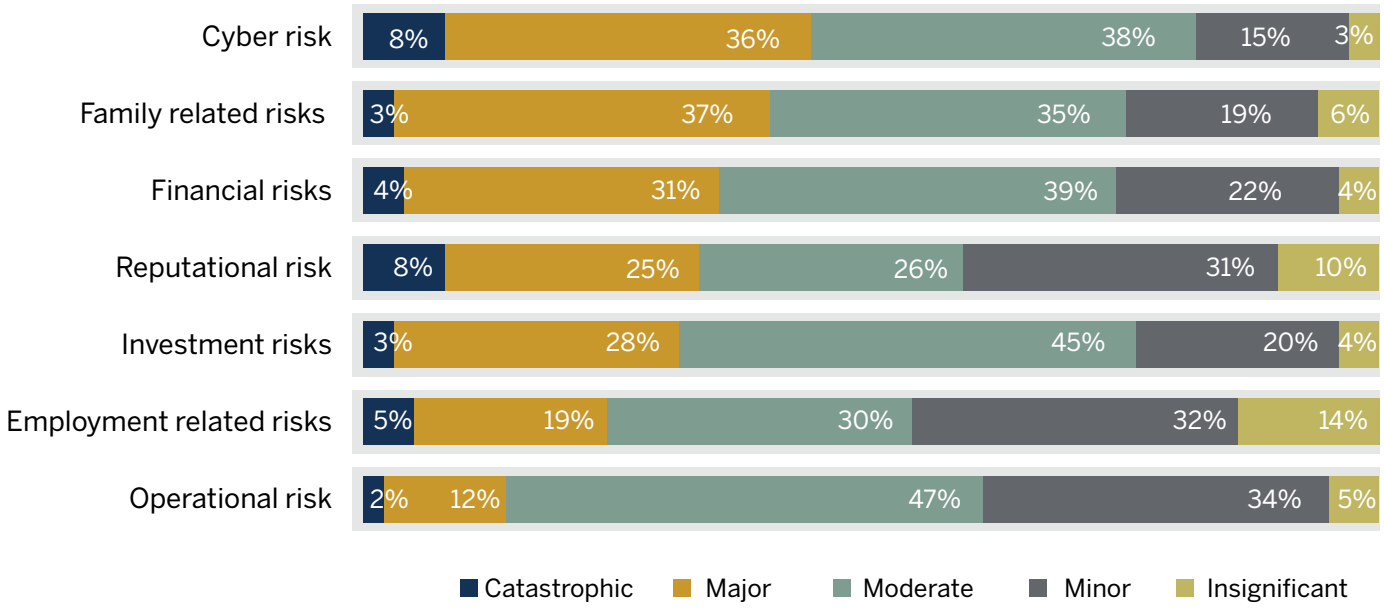
Along with the likelihood of a risk, its potential impact is important when assessing the overall threat level of a risk. Here, many family offices see cyber risks, such as a compromise of data confidentiality, integrity or availability, as having the potential to have a catastrophic or major impact. While a relatively low 8% think cyber risk would have a catastrophic impact if it materialized, 36% believe it would have a major impact and another 38% think it would have a moderate impact.

The results show that cyber risk has the biggest potential impact on family offices, should it materialize, ahead of family related risks, financial risks and investment risks.

For family office risk management, risks with a high potential impact need to be addressed, particularly if they also are likely to materialize. As cyber risk falls into both these categories, family offices are right to see it as one of the biggest risks they face.

The Potential Impact of Cyber Risk and Other Risks

If the following risks materialized, how much of an impact would they have on your organization?



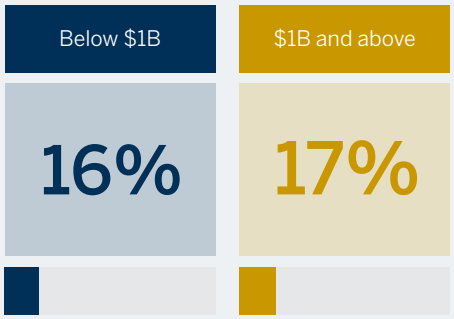
Looking at the findings on the potential impact of various risks by the age of family offices, it is clear that newer family offices see family related risks as being less likely to have a major to catastrophic impact than older family offices. Just under a quarter of family offices in existence for three years or less agree that family related risks would have a major to catastrophic impact, compared to almost half of family offices in existence for three to ten years and nearly 40% of those in existence for more than ten years. This is probably because newer family offices have not been through a family related risk event, while older family offices have seen the potential impact.

One of the best steps we took to bolster our own internal cybersecurity was having a cybersecurity company we acquired come run an assessment on our firm. They worked with us to set up internal protocols and technology to provide greater protection within our cyber infrastructure. We have found a huge benefit by surrounding ourselves with industry experts who understand and traffic in cybersecurity and cyber risk.

– Ward McNally, McNally Capital, LLC

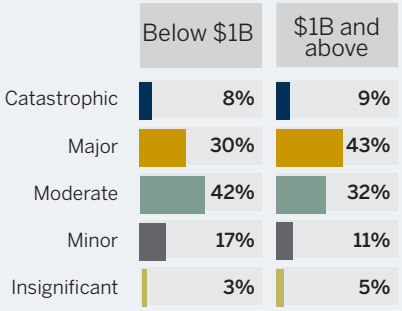
Smaller Family Offices by Asset Size Underestimate Cyberattacks

Despite facing a similar number of cyberattacks in the last year...

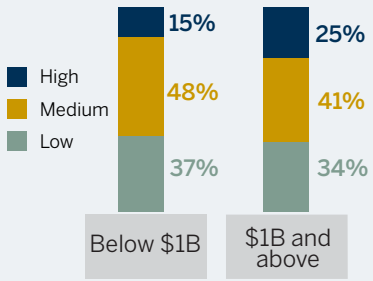


...smaller family offices underestimate cyberattacks - both its impact and likelihood.

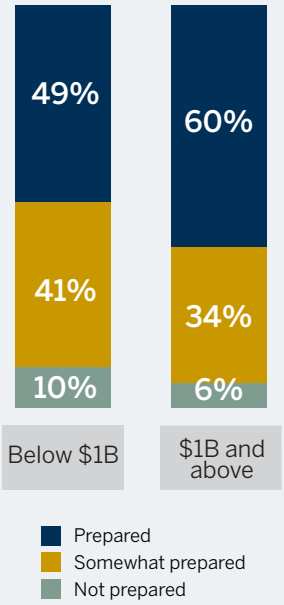
Impact of cyberattack



Likelihood of cyberattack



Smaller family offices are less prepared to handle risk.

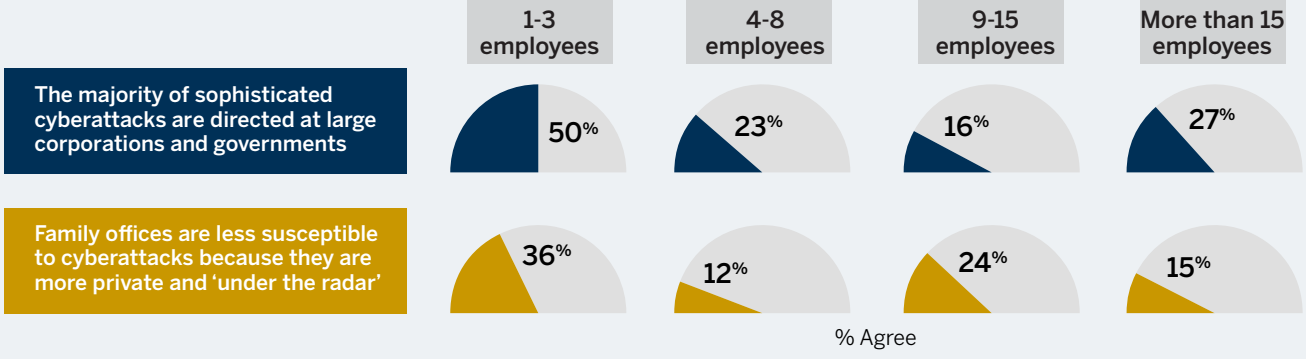


Cyber risks also rank lower than investment risks for smaller family offices.

Below $1B	
Investment risks	59%
Cyber risk	52%
Family related risks	52%

$1B and above	
Cyber risk	62%
Family related risks	60%
Investment risks	46%

Smaller family offices, in terms of staff members, have differing viewpoints from larger family offices.



While cyber risk is undoubtedly a big risk for family offices, it can vary widely in severity. At one extreme, family offices are highly likely to face relatively crude phishing attempts, where individuals are sent an email which encourages them to click on a link, which will then lead to a security breach. Sometimes 'phishing' is easily spotted, but cybercriminals rely on the law of averages eventually working in their favor, such as at times when an individual's guard is down. This type of cyberattack can be made much more dangerous if cybercriminals take over the email account of a family office principal, or someone known and trusted by family office staff, and use this to send out emails to individuals inside or outside the family office organization.

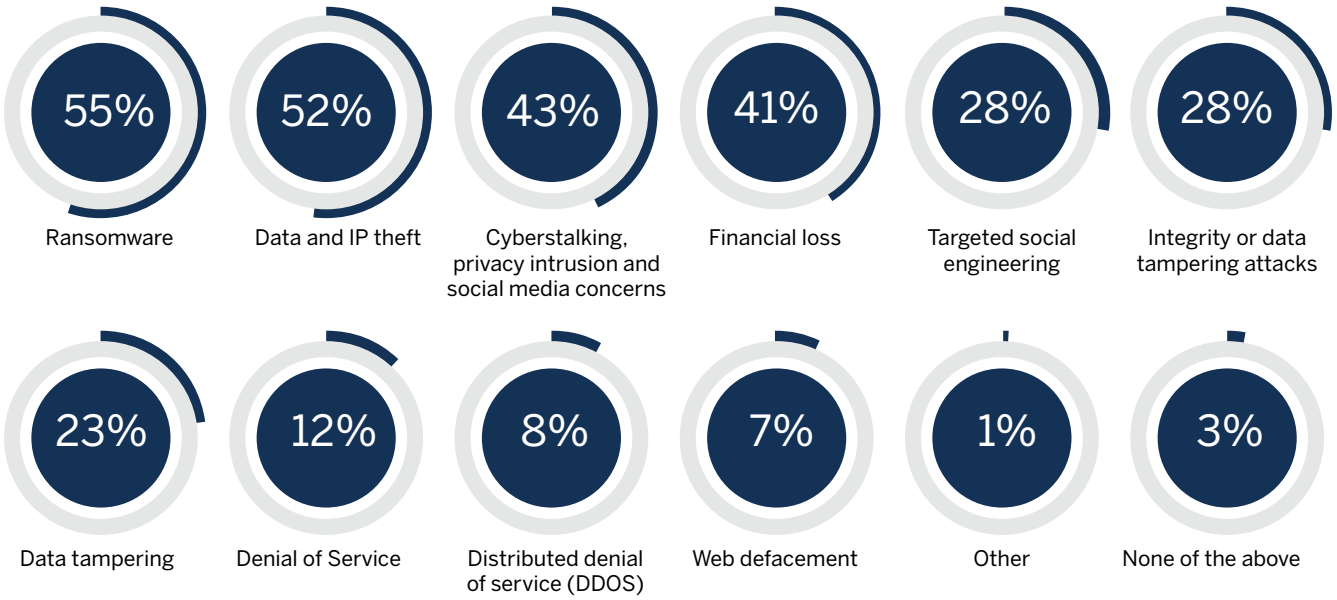
When asked to assess the different types of cyberattacks they face, ransomware is seen as the most likely cyber incident. This is concerning, because this type of cyberattack can be carried out by more sophisticated cybercriminals who have spent time studying potential victims to find loopholes in their IT systems and to ensure that they have the funds to pay a ransom, should the attack succeed. Typically, having breached their victim's defenses through a phishing email or other approach, hackers seize control of vital data files and deny access to them unless a ransom is paid, usually through bitcoin or a similar online currency.

Data and IP theft is also seen as a likely threat by family offices, with 52% citing this, ahead of cyberstalking, privacy intrusion and social media concerns (43%) and financial loss (41%). As family offices serve the needs of wealthy individuals and families, it is not surprising that cyberstalking and privacy concerns rank highly as cyber threats. Cyberstalking can be carried out for financial gain, or for revenge, harassment or bullying reasons, or even for ideological reasons.

Financial institutions are now among the prime targets of cybercriminals, whether it is to hack into the payment systems at banks, to steal personal data from credit card companies, or to trick organizations such as family offices into making a wireless transfer to a cybercriminal. Here, the increased use of remote working following the COVID-19 pandemic could increase the risks of financial loss, as weaker internal controls and an enlarged IT perimeter could be features of extended remote working.

Cyber Incidents Likely to Be Faced by Family Offices

What kind of cyber incidents do you think your family office is most likely to face?



% Yes, Multiple answers allowed

Family offices associated with an operating business say they are more likely to face cyberstalking, privacy intrusion and social media concerns, than those without an operating business (51% versus 33%). They are also, in their eyes, more likely to face targeted social engineering (33% versus 23%). One factor here is that family offices associated with an operating business may have a higher overall public profile, if the operating business is known to the general public. This in turn may increase risks from threats such as cyberstalking as more information about the family may be in the public domain.

At the same time, family offices associated with an operating business may also be able to make use of the resource of the operating business in countering cyber risks. This is in line with the finding that family offices associated with an operating business are more likely to have countered risks by training employees and family members about risks (64% for family offices associated with an operating business versus 51% for family offices not associated with an operating business).

Security Incidents at Family Offices

Threats to Family Offices

Can you provide specific examples of any risks, threats, security incidents or suspicious activity that your family members or family office clients have faced in the past 5 years?

"We experienced a sophisticated cyberattack from hackers based overseas. They accessed family office data through a server we shared with the operating company, which was also hacked. The hackers wanted us to pay a ransom, or they would release confidential data to cyber criminals. We refused to pay a ransom and stopped the security breach."

"The most serious cyberattack we experienced was when someone posed as one of the principals and asked for a bank transfer to an overseas account. What made it worse was that the principal concerned was travelling at the time and the hacker sent an email from what appeared to be the principal's account. However, because we employ multiple checks on all payments, we managed to detect the cyberattack and prevent it from succeeding."

"We have had several unsuccessful attempts by outside parties to pose as employees and have us wire money to them."

Misalignment of Needs and Services

A Need for a Better Coordinated Set of Risk Management Services

With cybersecurity among the top risks, it is a little surprising then that less than half (47%) of family offices offer cybersecurity as a risk management service. In addition to cybersecurity, insurance (68%) and legal services (51%) are among the top risk and threat management services implemented by family offices as part of their operations.

However, few family offices provide holistic risk and threat management services. Critical services like privacy and reputation management, physical security, international travel and personnel evaluation and monitoring are provided by only about a quarter of family offices.

Risk and Threat Management Services Implemented by Family Offices

Which of the following risk and threat management services do you implement as part of the family office operations?

International Travel and Health Advisory Services are Critical Risk Services but Infrequently Implemented by Family Offices

The survey data suggests that family offices have developed strong risk management mechanisms within the financial risk management domain. However, much more common is the major disruption of family affairs and continuity due to significant health issues or untimely death. Yet only 16% of respondents of the survey indicated that they hire professional management for their health care risk management.

Today, the tools one has to manage health risk and significantly increase longevity are now actually better than the financial risk management tools used to protect wealth. Private health advisory for family offices offers an array of sophisticated tools for preventive diagnostic health assessments, carefully coordinated major case management and global coverage in case of emergency.

> *Rapid innovation in medicine has created an amazing opportunity to reduce health risk and measurably extend healthy life. However, the same rapid innovation cycle creates information and health system navigation gaps that leave even sophisticated family offices struggling to choose optimal solutions.*
>
> –John Prufeta, Medical Excellence International

How Family Offices Are Tackling Cybersecurity

Given the increasing risks of cyberattacks on family offices, there is an urgent need for family offices to implement cybersecurity measures to protect themselves. This has been addressed to an extent, although it is clear that more can, and should, be done.

For example, 72% of family offices have trained staff on how to work properly and securely in a remote environment. Given that the COVID-19 pandemic has led to most investment professionals having to work remotely, this is a basic requirement for family office personnel. If over a quarter of family office staff have not been trained in working safely from a remote location, this represents a potential vulnerability at this time.

A similar number (69%) say that they actively manage all hardware and software on the family office network. Again, while it is good to see that this is being done by most family offices, it means a significant number are not doing this. As remote working during the pandemic could lead to family office personnel using new devices and software, it is more important than ever to maintain network security at family offices.

Around half of family offices use a variety of cybersecurity measures, including:

- Requiring staff to participate in periodic cybersecurity training (55%).
- Using consistent endpoint protection (54%).
- Working with a third-party vendor on investigating urgent security incidents (51%).
- Developing a cybersecurity incident response plan (50%).
- Mapping or identifying all personal data on family office systems (46%).
- Conducting penetration tests of the family office IT network in the past year (46%).
- And keeping and using an audit log of IT system events (46%).

While it is good that these cybersecurity measures are being used, it could be argued that they should be used by virtually all family offices.

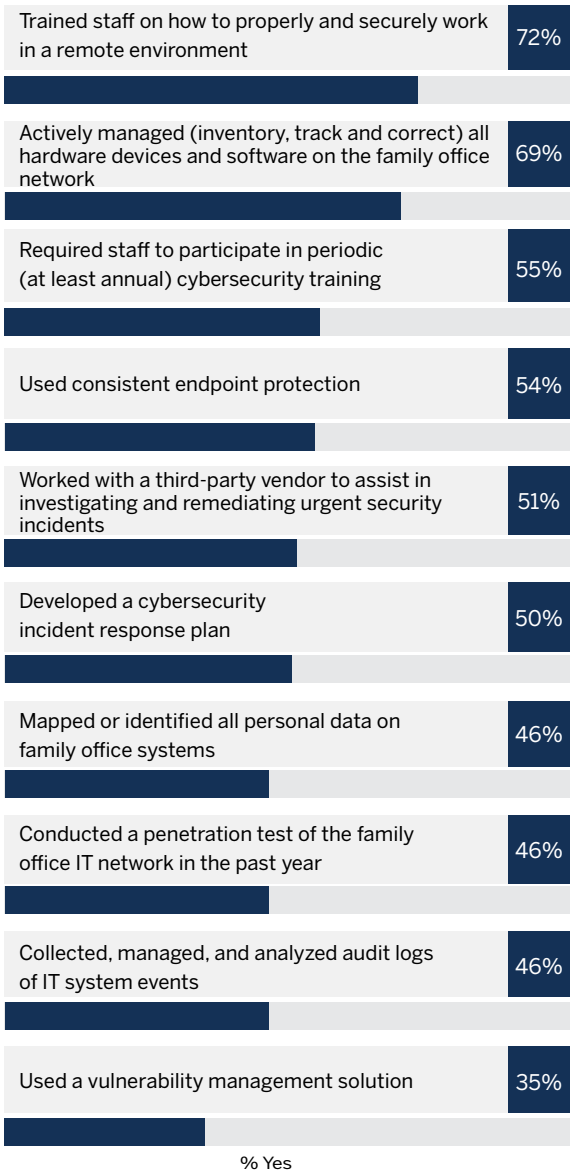
It is also surprising that only just over a third (35%) of family offices say they have used a vulnerability management solution. Whereas firewalls and antivirus software tools defend a network against attack on a reactive basis, a vulnerability management solution will actively look for weakness in a network and then take remedial action on a priority basis to reduce or eliminate vulnerable areas in a network. It is therefore a more proactive approach to assessing and managing cybersecurity and should be used more widely by family offices.

Looking at the age of family offices, it is clear that older family offices, in existence for more than 10 years, have generally taken more cybersecurity measures compared to newer family offices, with less than 10 years' existence. For example, older family offices are more likely to have developed a cybersecurity response plan (60% for older family offices versus 31% for newer family offices), collected, managed and analyzed audit logs of IT system events (56% versus 33%), required staff to participate in periodic cybersecurity training (62% versus 44%), and mapped or identified all personal data on family office systems (53% versus 36%).

These differences are likely a reflection of a more structured and comprehensive risk management approach at older family offices, which is very likely to be due to their greater experience and resources. Family offices that have been set up more recently are more likely to be concentrating on investment and financial risks as priorities, as they commence operations. But these newer offices still need to take action on cybersecurity, as it is a major threat to all family offices.

Cybersecurity Measures

Has your family office taken any of the following cybersecurity measures?



81% of family offices fail to conduct periodic background checks on personnel

Family Offices Fail to Carry Out Regular Background Checks on Staff

Insider threats stem from legitimate users who have approved access to computer systems in an organization. Threats from insiders can develop from either nefarious intent to cause harm to networks or from unsuspecting staff or family members who unintentionally compromise information systems or leak data. Insider threats can also come from former employees or third parties who have regular or privileged access to systems.

In the family office context, it is quite common to see employees with outsized access to information because of the lean staffing nature of most family offices. Combined with a focus of efficiency of operations over effective security and the low resource allocation to IT and security functions that family offices encounter, insider threat issues are abundant in the family office world.

Moreover, detecting insider threats is not easy. They already have access (sometimes privileged access) to systems, they have valid access to systems, and determining the difference between malicious or nefarious activity versus regular activity can be difficult.

The study presented some interesting results on insider threats that should be examined further in future research, especially insider threats resulting from family members.

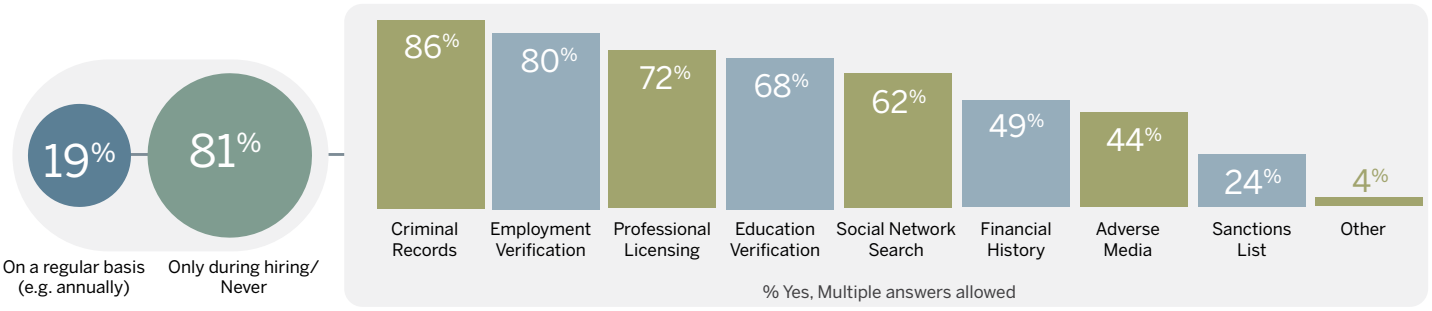
Personnel evaluation and monitoring is another critical service offered by only 28% of family offices. Of note, 81% of family offices fail to conduct regular background checks on family office staff. While 68% of family offices conduct background checks on hiring, most of them neglected to conduct follow up evaluations which creates a large source of vulnerability for family offices. More than one in ten (13%) never conduct background checks.

Only one in ten (12%) cite employee related/insider threats to be among the biggest risks facing family offices and a quarter say their impact will be catastrophic or major. Only 17% think these risks are likely.

Of those who conduct background checks, the data they are most likely to review are criminal records (86%), employment verification (80%) and professional licensing (72%).

Family Offices Check Criminal and Employment Records During Background Checks

You mentioned you conduct periodic background checks on all staff, what data do you review?



Insider threat is also part of the "concentric rings of security" that are needed to be addressed by many family offices. This is rarely talked about but is a serious threat. There are many technologies and strategies available today that can help with this issue.

– Mike Janke, DataTribe

Tail Risk Is a Key Focus for Family Offices

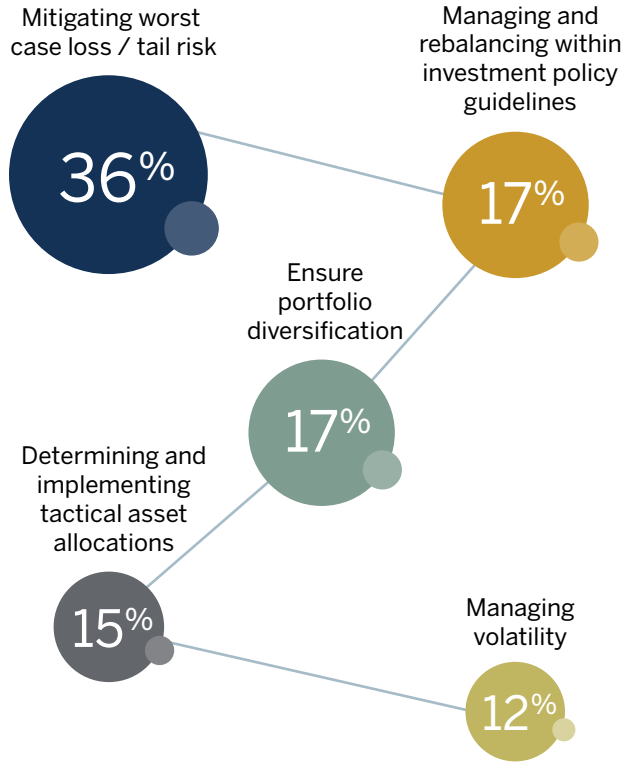
Investment risk, such as the potential of incurring losses due to movements in market prices, is a fundamental area of concern for family offices. Here, the results show that mitigating worst case losses, or tail risks, is a primary focus for over a third (36%) of family offices, more than twice the rate of any other category of investment risk. This is logical, as wealth preservation and accumulation are likely to be key components of the overall investment objectives for family offices. Tail risks, or risks with a relatively low likelihood but devastating consequences, are therefore a major concern for family offices. As a result, investment portfolios need to be thoughtfully managed to substantially reduce the likelihood of a tail event, and to minimize the economic impact if they do occur. One possible tail risk is a severe and unexpected drawdown in equity markets. To manage against this risk, family offices might choose to implement hedging strategies to mitigate losses, or to diversify across a broad range of asset classes and investment strategies, including those that have low to negative correlation to equities, which could perform well if equity markets suffer a sharp decline.

Following the reduction of tail risk, family offices see disciplined portfolio management as vital for managing investment risks. Seventeen percent of respondents say managing and rebalancing within investment policy guidelines is a primary focus, and the same proportion state that ensuring portfolio diversification is a main objective. A slightly lower number (15%) say that determining and implementing tactical asset allocation decisions is important to successfully handling investment risk, while 12% see managing volatility as a key focus for investment risk management.

Portfolio diversification, as well as managing and rebalancing within investment policy guidelines, are cornerstones for a disciplined approach to investment management, helping to reduce investment risk over time. Additionally, tactical asset allocation can also assist family offices in avoiding or mitigating losses in particular market sectors or asset classes, with the added potential of benefitting from short-term opportunities.

Managing Investment Risk at Family Offices

What is your primary focus when considering investment risk in the portfolio?



Reputational Risk is Neglected by Most Family Offices

Privacy and reputation management is crucial to family offices since they are intrinsically private by nature and have a lot to lose if principals were to have their reputation tarnished. Reputation has flimsy foundations in that a life's worth of hard work and effort can be shred easily with something small and seemingly innocuous – a misplaced social media post or comment, or a stolen email address or personal connections. Yet only 28% of family offices offer this service; hardly surprising since only 26% consider reputational risks among the biggest risks to family offices, only a third think they present major or catastrophic impacts and three quarters (72%) think they have a low chance of occurring.

Other services like physical security and international travel are also provided by few family offices. Needless to say, physical security is paramount and family offices need to protect the principals from direct physical threats, such as kidnapping, break-ins, etc., and implement the concentric rings of security. Travel security has its own set of challenges for family offices.

Family Offices Need to Look to Outside Risk and Threat Expertise

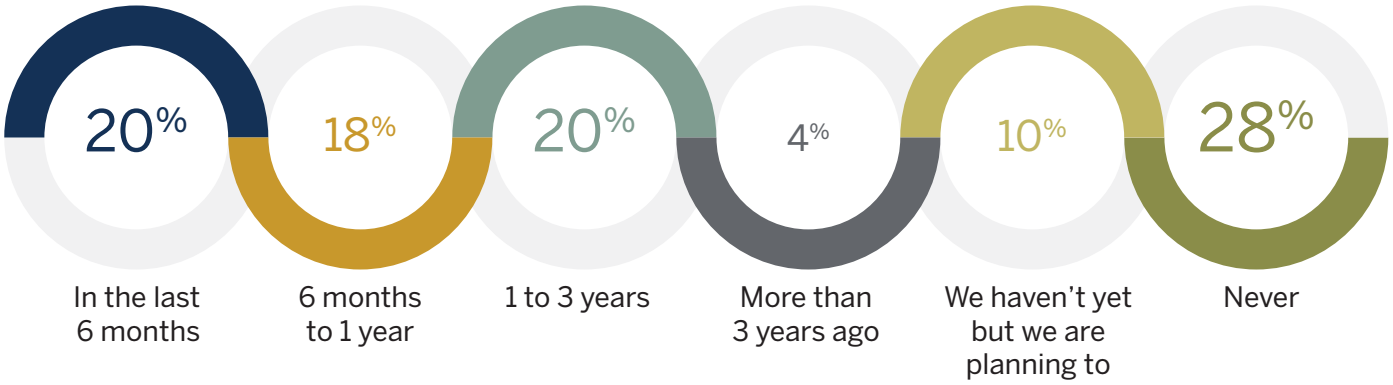
The failure of family offices to use third-party security experts was a very interesting finding of this report. It underscores the importance of education of principals and staff on this critical topic for two reasons: family offices are usually not large enough to warrant staffing with risk and threat experts with relevant experience and the evolving nature of threats that family offices face requires outside expertise and updated technology solutions. When you add the complexities of remote working (even if temporary during a crisis), the need for specialized expertise becomes even more important.

Approximately two in five family offices have not conducted a review of the risks and threats to family office members using a third-party vendor, with 28% never conducting a review and 10% planning to do so.

Two-fifths (38%) have managed to conduct a review in the past year while a fifth (20%) have done so in the past one to three years. Just 4% last did a review more than three years ago.

Review by Third-Party Vendors on Risk and Threat

When was the last time your team conducted a review of the risks and threats to family members or family office clients using third-party vendor?



Many family offices tend to evaluate their risk and threat exposure within a functional silo, such as cybersecurity, without considering or contemplating how enterprise risks are amorphous and can often extend across functional boundaries. A myopic assessment of functional risk often results in unrecognized gaps and vulnerabilities – only discovered in the course of an actual incident or risk event. Enterprise risk mitigation is a team sport requiring a bench of diverse skill sets, tools and strategies.

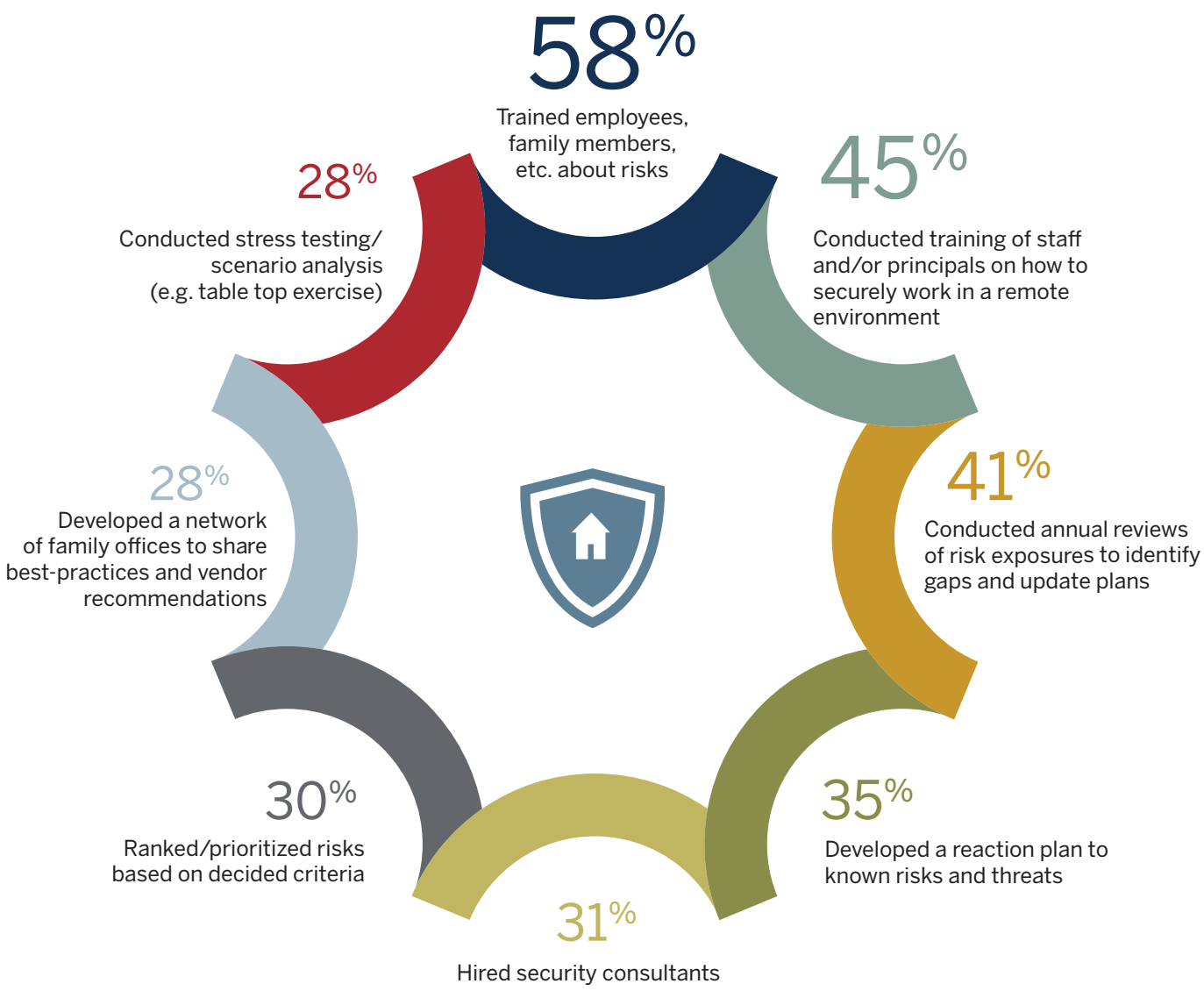
– Wesley S. Bull, Mantle Advisors LLC

Family Offices Use Training to Counter Risks – But Is It Enough?

In order to counter risks to their family office, more than half (58%) of respondents have trained employees, family members and others about risks. More than two in five also conducted training on how to securely work in a remote environment (45%) and conducted annual reviews of risk (41%).

Steps to Counter Risks

Which of the following steps, if any, have you taken to counter risks to your family office?



% Yes, Multiple answers allowed

Family Offices and Their Use of External Vendors

Balancing the Need for Outsourcing

Family Offices Tend to Insource Financial Risk Personnel and Outsource Cybersecurity-Related Risk Services

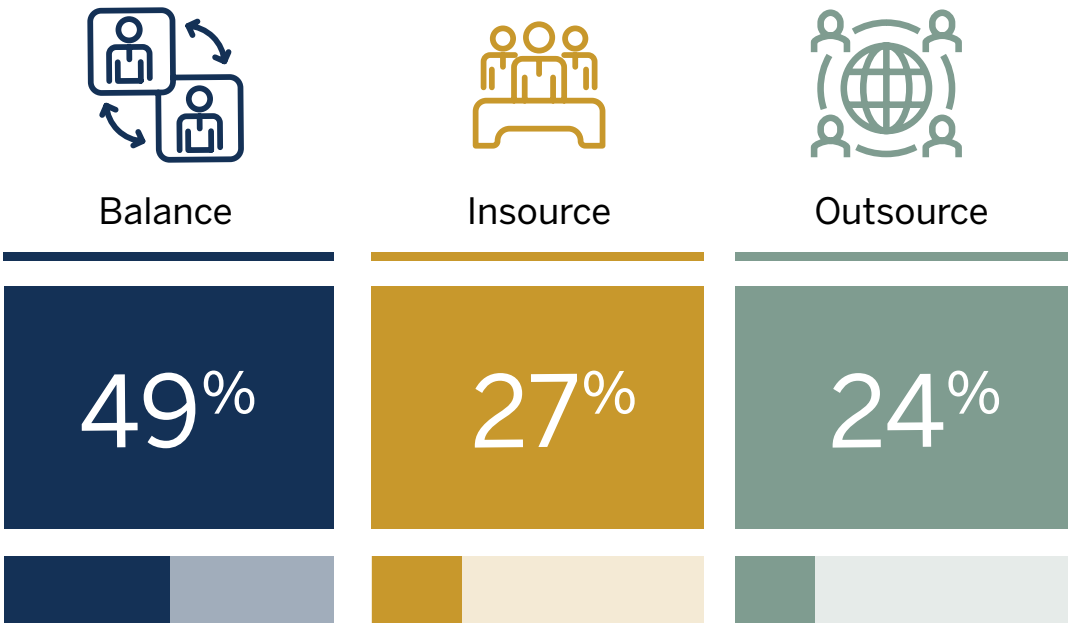
For risk management, smaller organizations such as many family offices, have to decide to what extent they outsource or insource key services. Around half (49%) strike a balance here between insourcing, where they possess the expertise, and outsourcing, where external vendors can provide a better or more efficient service.

The remaining family offices are fairly evenly divided over insourcing and outsourcing, with slightly more (27%) saying that they tend to insource, compared to 24% who tend to outsource.

As even very large financial institutions will use external providers for some services, it is not surprising that just under three-quarters of family offices, which are by their nature smaller, will either take a balanced approach, or tend to outsource the services they need. Where insourcing is the norm, it is likely to be at larger family offices or where they operate on a relatively simple basis. But even in these situations, these family offices may be taking risks if they rely on internal staff who may be overburdened with work, or who have to undertake tasks they are unqualified for.

Family Offices and the Insourcing Vs. Outsourcing Decisions

Do you tend to more frequently insource or outsource all services in your family office?



Family Offices Are Increasingly Training Staff on Potential Risks but More Rarely Have Plans or Stress Test Those Reaction Plans

Looking at where family offices use internal resources and where they outsource, the results show that financial risks are more likely to be handled internally, while cyber risks are more likely to be outsourced. For example, 35% of family offices have specialized internal risk management teams or personnel for financial risks and a further 39% handle financial risks internally but without specialized teams or personnel.

And while 32% of family offices outsource cyber risk management to external vendors, only 12% do this for financial risks. Nevertheless, half of the family offices in this research address cyber risks on an internal basis; 30% of them do this without specialized teams or personnel, while 20% do have specialized risk management teams and personnel.

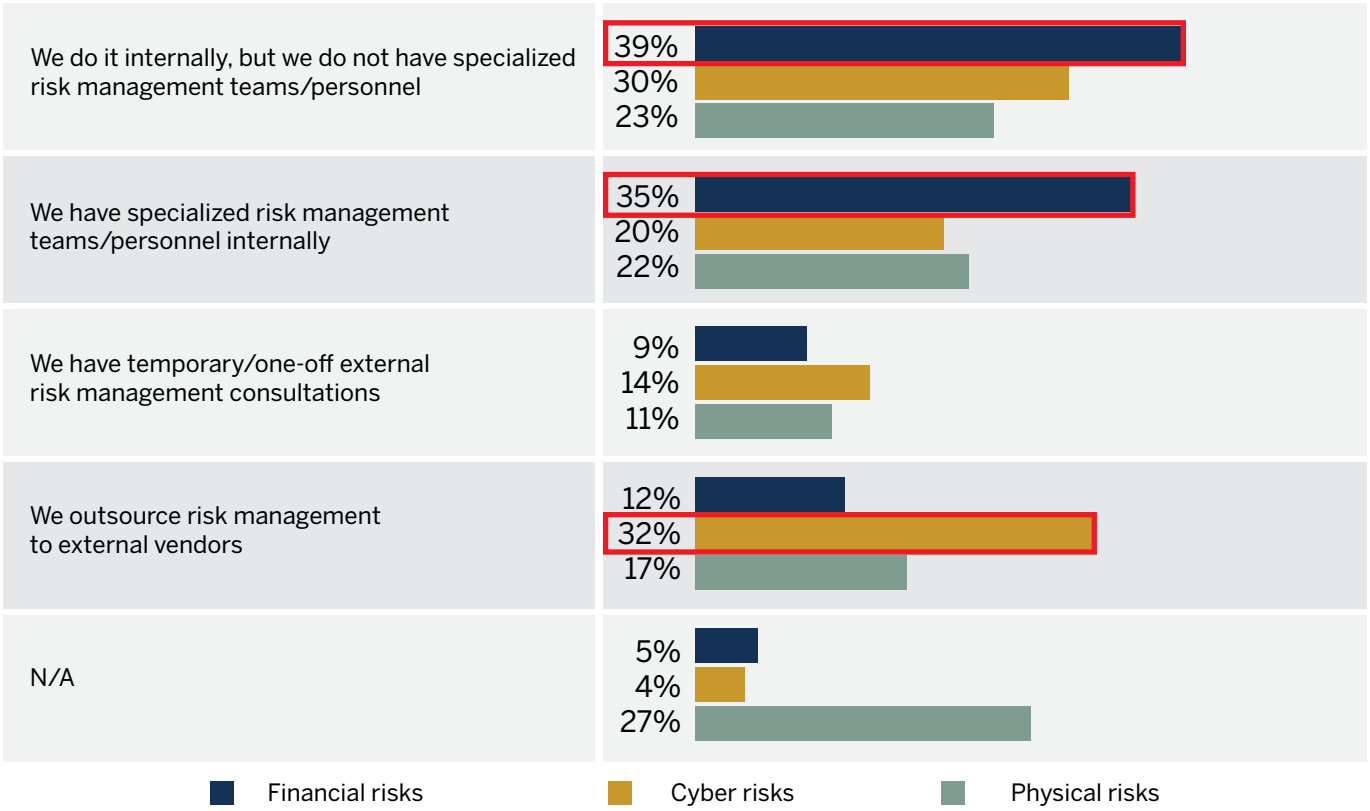
Based on these findings, family offices are more likely to make use of external vendors for physical risks than for financial risks, but less likely to do this compared to cyber risks. Under half (45%) of family offices handle physical risks internally, while 28% either use external vendors on a one-off or temporary basis, or as a longer term outsourced vendor. And just over a quarter (27%) do neither, as they do not see physical risks as applicable to their family office.

Generally, these findings show relatively low use of external vendors for risk management. In particular, there is relatively little use of temporary or one-off external risk management consultations, with only 9% of family offices doing so for financial risks and only 14% for cyber risks.

Given the range and potential severity of cyber risks, there is scope for family offices to make more use of external vendors, either for one-off consultations or for ongoing risk management. Eight out of ten (80%) family offices lack internal specialized risk management teams or personnel for cyber risk and less than half (46%) use external vendors. This means there are vulnerabilities at a number of family offices where risk management for cyber risk is either addressed by internal staff who lack specialized risk management skills (30% of family offices), or it is only covered on a temporary or one-off basis by external risk management consultations (14%).

How Family Offices Address Different Risks

How does your organization address risk management for the following types of risks?



Effectively Using External Vendors for Risk Management Can be a Challenge for Family Offices

While family offices can be criticized for failing to use external vendors for risk management purposes, they do face a number of challenges in finding and using them.

The most common challenges for family offices are not knowing where to find good external risk vendors and a lack of external vendors with tailored approaches for family offices (both 35%). This is followed by concerns over privacy (34%) and on the oversight of external vendors, such as evaluating and managing their work (33%). These concerns make it easier for family offices to justify relying on internal resources for risk management.

Several other issues are also seen as challenges when using external vendors, including a lack of data and information on external vendors (25%) and risks such as poor performance and data theft when using external vendors (20%). These concerns all reinforce the fact that for external vendors to add value to family offices in risk management, they need to be properly selected and managed, with their work assessed and with good oversight and communication. If this is not the case, then using external vendors could fail to provide a viable risk management solution for family offices.

For external vendors with skills in managing cyber risks, these findings show that family offices may not know how to find them, or may feel their services are not tailored to meet the needs of family offices. Vendors also need to reassure potential family office customers that they can meet their needs when it comes to privacy, performance, data security and other issues around working with family offices.

Family Offices on Their Challenges With External Risk Vendors

What are the top challenges you face with using external risk vendors for risk management?

% Yes, Multiple answers allowed

Choosing the right risk and threat management vendor remains a large challenge for family offices

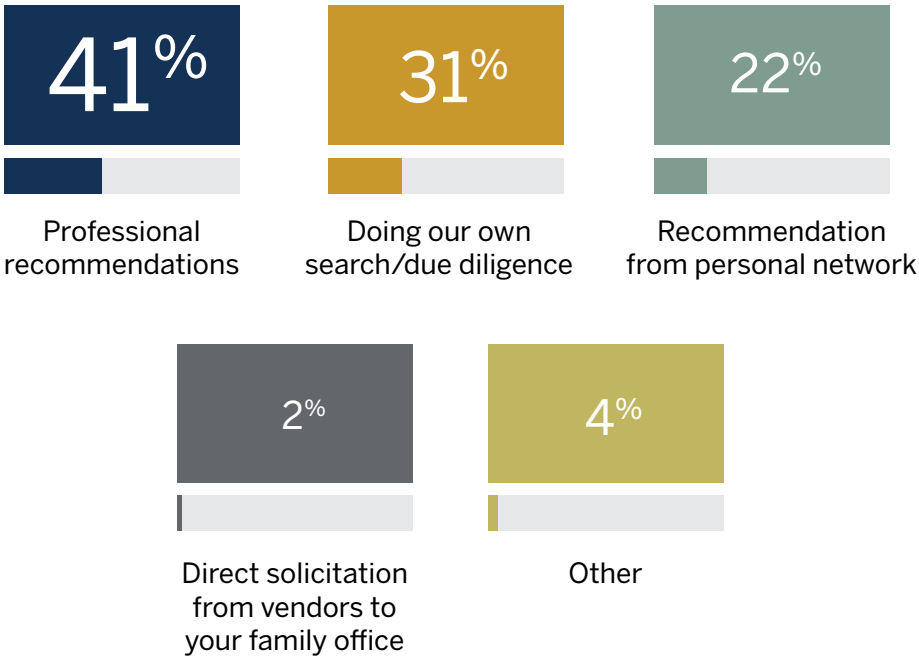
Given that over a third (35%) of family offices have said they have difficulty in finding good external vendors, it is not surprising that professional and personal recommendations are important when family offices select cyber and physical risk management personnel. More than four-in-ten (41%) of family offices use professional recommendations to select vendors, while over a fifth (22%) use recommendations from their personal network, such as family and friends. Nearly a third (31%) do not use recommendations but do their own research and due diligence when selecting external vendors for cyber risk and physical risks.

All of these methods of selecting vendors have their merits. Professional recommendations from lawyers or private bankers can give reassurance over the credentials of an external vendor, while experienced family office staff may have extensive personal networks they can tap into. In either case, using proper selection criteria and carrying out due diligence is important to ensure that an external vendor is suitably qualified. Relying solely on the recommendations of others can leave a family office open to an unhappy experience should the vendor lack the right skills and experience, or be unsuited to the needs of a particular family office.

Cyber risks are an emerging threat and constantly evolving, as hackers and cybercriminals adapt to the cyber measures taken by organizations, so relying on recommendations based on past experience might not be the best strategy. As well as considering what external vendors for risk management have done in the past, family offices need to look at how likely a vendor is to be able to cope with future threats, as and when they materialize.

Selecting Risk Management Personnel or Vendors

How did you select your cyber and physical risk management personnel or vendors?



Plugging the Knowledge Gap

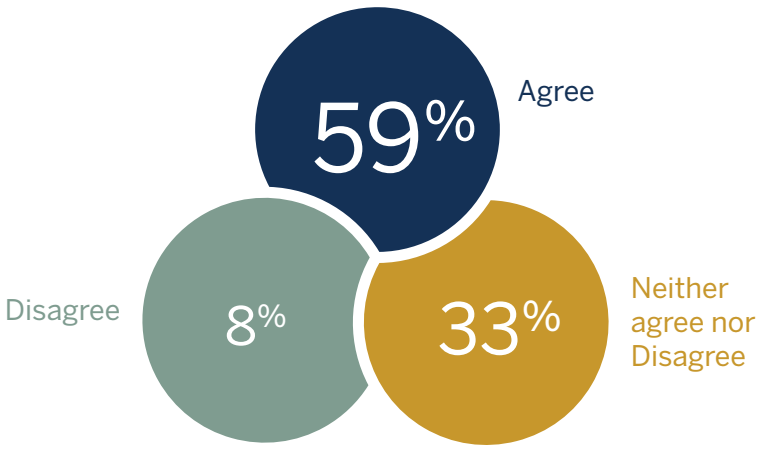
There is a need for a strong peer network of family offices centered around risk

As many family offices see cyber risk as an important issue, but lack knowledge about suitable vendors and wider issues about cybersecurity, there is need for family offices to learn more about emerging threats and the best risk management practices. As a result, nearly six-in-ten (59%) respondents agree that there should be more conferences where family offices can network and learn about emerging threats and risk management best practices, while only 8% disagree with this.

While the COVID-19 pandemic is still an issue, family office staff and others are unable to attend physical events and so will have to attend virtual conferences. These can offer a good way to learn but lack informal networking opportunities which can be useful. But if the risks of COVID-19 recede in the future, then conferences and seminars could be valuable ways for family office staff to learn more about emerging threats and risk management best practices from experts, and also connect with their peers at other family offices and share views and experiences with them.

Addressing the Knowledge Gap

There should be more conferences where family offices can network and learn about emerging threats and best risk management practices



When participating in a network of family offices, the participant should consider the operating demographics of the network's other participants. Optimally, a network should include diversity in operating demographics so that relevant best practices can be shared in order to increase the chances of identifying novel risks.

–Brad Deflin, Total Digital Security

Practical Tips and Recommendations

This report highlights some of the critical areas where family offices need to improve their existing risk and threat management planning and operations. 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.

We provide this list as a set of recommendations that family offices can leverage to improve their positions:

- Conduct a risk baseline assessment using a qualified risk and security consultant with direct experience working with family offices. Conduct at least annual evaluations after the initial assessment.
- Conduct initial background checks on all family office employees and develop mechanisms of working with legal and risk experts to monitor and conduct follow up background checks for existing employees.
- Work with healthcare advisory experts to develop and test plans around disruption of family affairs and continuity due to significant health issues or untimely death.
- Risk and threat management for family offices is a specialized area that requires professionals with applicable experience. For example, cybersecurity expertise is not the same as information technology expertise.
- Intelligence on all risks is important. For example, there are a number of cyber products available that can monitor and provide intelligence from the dark web, social media and signals coming from outside your network.
- Insist on working with vendors that go beyond "desktop due diligence" which rely solely/heavily on open-source/public information whether evaluating the family office or conducting due diligence on deals.
- Evaluate current risk and threat management providers regularly to see if service upgrades or additional help is warranted.
- Proactively discuss the annual budget for the family office allocated to risk management.
- When choosing vendors, consider the benefits of attorney-client privilege as part of a comprehensive risk and threat management strategy.
- Have crisis plans for specific scenarios (death of a principal, cybersecurity breach, social media bullying, confidential information is being leaked) and practice it.
- Keep a log of risk and threat issues the family or family office has faced in the past.
- Develop and practice continuity of operational and disaster recovery plans for physical, financial, and digital assets.
- Evaluate insurable exposures regularly and during changes in the family and/or business and ensure comprehensive understanding of terms and conditions current coverage.
- Protect the devices used for business, even if it is an employee-owned device, with monitored and managed end-point security.
- Secure the local (home, home-office) ISP network including a virtual private network (VPN) for outbound communications.
- Train and test the employees regularly on risk and threat issue identification and mitigation and review policies and procedures for employee duties and responsibilities as they pertain to information security.

- Develop networks with other family offices to share best practices and vendor recommendations.
- Inventory all devices used to access the internet; computers, laptops, phones, iPads, and tablets and maintain a list of all networks used by family members and family office staff.
- Identify all email addresses used by family members and family office staff.
- Use autonomous end-point security systems and install VPN apps to each mobile computer and smartphone.
- Employ SD-WAN security systems for comprehensive and autonomous protection of fixed-networks and devices.
- Generate and test policies for work email and internet browsing and privatize personal mail.
- Use two-factor authentication for applications whenever possible.
- Avoid easy to guess passwords, change passwords regularly, and use different passwords for different services.
- Back up data regularly and in multiple ways (on and off-site).
- Leverage password manager solutions to avoid using the same password for multiple services.
- Keep software updated on mobile and non-mobile devices.
- Use encrypted mail for sending any personal or sensitive business information (due diligence data, account numbers, family financials, credit card numbers, addresses, investment details, birth dates or social security numbers, etc.).
- Work with legal counsel to develop and execute non-disclosure agreements with family office staff.
- Identify, document, and review signatory procedures throughout the family office.
- Assess and test internal controls with accounting firms that have experience working with family offices.
- Review family office policies to ensure compliance with federal, state, and local laws.
- Develop and maintain a document collection and management process that is applicable to current and potential future family office requirements.
- Plan and conduct table top exercises ("simulated war games") with relevant family members, family office staff, and external advisors.
- Develop, document, and practice a cyber and privacy "breach plan" with internal and external stakeholders.

Background of the Survey

Methodology

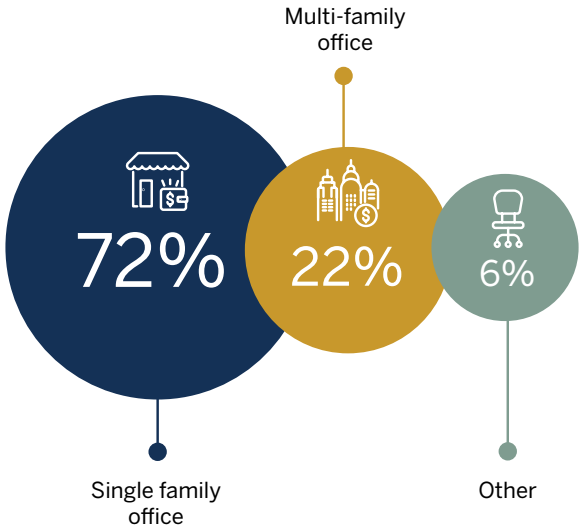
Data for this report was collected using an online survey among 200 family office executives. Data was collected from May 25th – August 10th, 2020. The survey was administrated by an independent research company, CoreData Research and the analysis of results were completed by Boston Private and our survey partners. Respondents were sourced from a mix of Boston Private and our survey partner databases.

Demographics

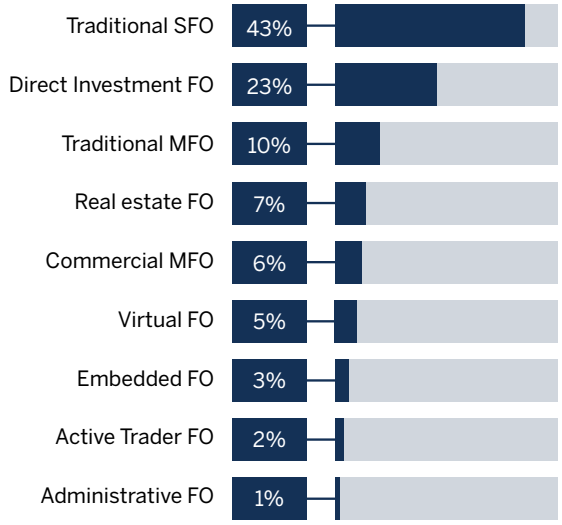
Respondents to the survey represented a diverse mix of family office archetypes. Below are some of the demographic highlights of our respondents:

- Most respondents were single family offices and described themselves as traditional SFOs.
- Most of the family offices were between $100mm and $5B in net worth (2% of family offices did not disclose their net worth).
- A majority of the family office executives had worked in the family office industry for more than a decade.
- Staffing size of the family offices was split quite evenly across the range with a slightly higher number of family offices with 4-8 staff members.
- Most of the family offices had been in business for 10+ years (60%) or at least 3-10 years (27%).
- Family offices were evenly split on the question of association with an operating business.
- Geographically, family offices were concentrated in the Northeast and Southern states of the U.S. with 9% international responses (Australia, Brazil, Canada, Europe, Germany, Hong Kong, Italy, Mexico, Peru, Portugal, Singapore, South Africa and United Kingdom).
- Most family offices served 3 generations or less and 19% served the original wealth creator.

Which of the following best describes the type of organization you work in?



What sub-type of family office (FO) would best describe you?



Commercial MFO: A business staffed with professionals that offer family office services. Sometimes executed through a discrete partnership and other times on an existing platform of a bank, financial services firm, accounting firm, or law firm.

Real Estate FO: Primary assets are real estate and tend to invest mostly in real estate assets. Family office functions are often embedded in the operating company and focus on managing the personal affairs of the principals.

Traditional SFO: Provide solutions over a broad range of service and advisory needs, historically through their own staff.

Traditional MFO: One family partners with a few other families to provide services to unrelated families; not designed as a commercial entity but more of an effort to share expenses and connect with a small number of like-minded families.

Embedded FO: Integrated into operating companies and usually provide family office services leveraging existing family business employees.

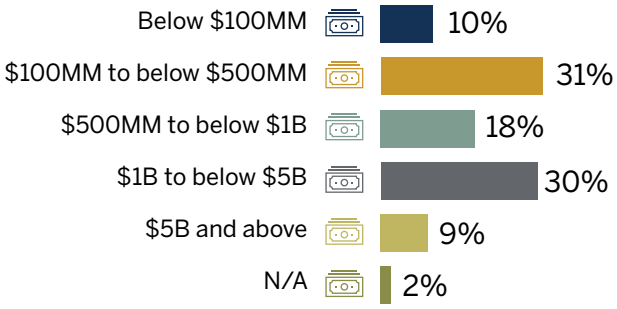
Virtual FO: Outsource staff as much as possible and family office service delivery coordinated by a single party (e.g. law firm, accounting firm, financial services firm).

Direct Investment FO: Focus their investment activities almost exclusively on private investing.

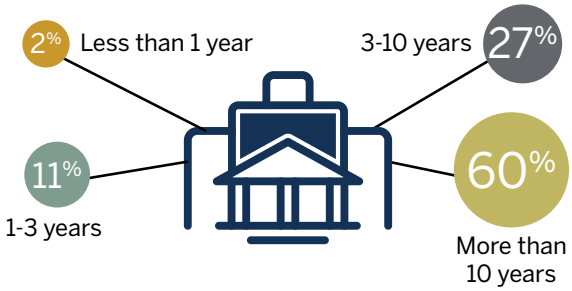
Active Trader FO: Typically larger family offices that focus on active investment strategies in liquid capital markets; e.g. former hedge fund managers.

Administrative FO: Limited generally to non-investment related activities. Focus their efforts on managing personal assets, administration, wealth education, among other areas.

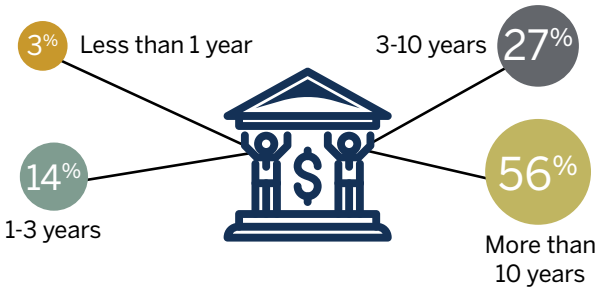
What is the cumulative value of assets over which your organization is responsible, including real estate and private investments if applicable?



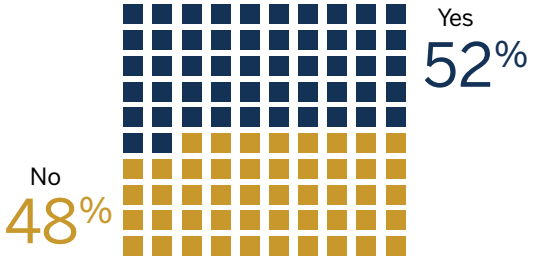
How long has your family office been in existence?



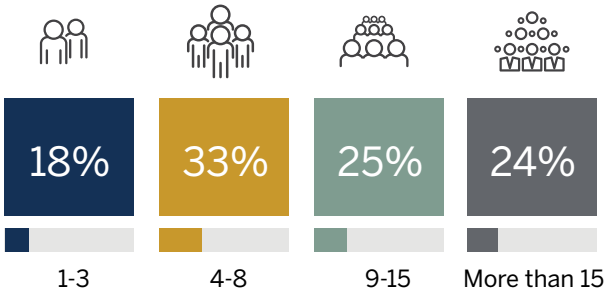
How long have you worked in the family office industry?



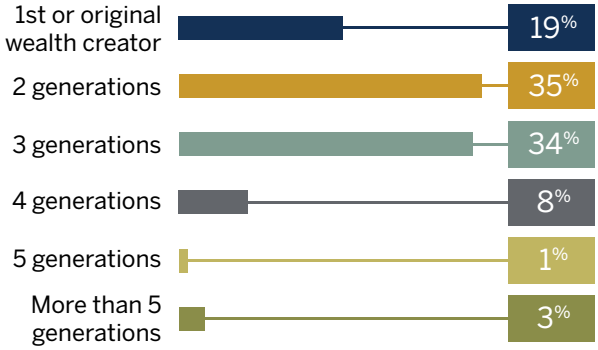
Is your family office associated with an operating business?



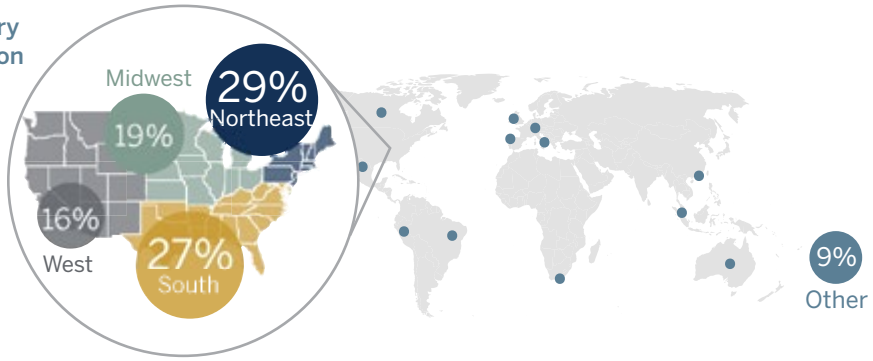
How many people work in your family office?



How many generations of family members do you serve at the family office?



What state in the US or country in the world is your organization located?



Our Survey Partners

Many thanks to our survey partners at The Chertoff Group, Dentons, McNally Capital, and Datatribe. Their teams supported the deployment of the survey. Our partners also lent their global expert insights into the risks and threats family offices face to support the development of the survey and learnings we were able to uncover with this research project. We look forward to future collaboration with our partners with a series of podcasts and webinars in October 2020.

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 the 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.

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.

For more information, please visit bostonprivate.com/familyoffice.