Deloitte.
Private

The Family Office Insights Series - Global Edition

The Family Office Cybersecurity Report, 2024

Interactive navigation

This report has been designed to deliver an interactive experience, which is available when opened in Adobe Acrobat.

If you do not have Adobe Acrobat, you can download it for free. Please note that without using Adobe Acrobat, some or all the interactive features may not be available.

Click here to download Adobe Acrobat

Contents

Foreword

Welcome to **The Family Office Cybersecurity Report**, which is the fourth edition of Deloitte Private's new **Family Office Insights Series**. This report offers invaluable insights into family offices' experience with cyberattacks, the means they are using to protect themselves, and what activities they can adopt to help safeguard themselves against future attacks.

The data in this report is based on a survey of 354 single family offices from around the world between September and December 2023. These offices oversee an average assets under management (AUM) of US$2.0 billion, while the associated families have an average wealth of US$3.8 billion. Collectively, this totals an estimated US$708 billion in AUM and US$1.3 trillion in family wealth (figures 1 and 2).

We also conducted 40 in-depth interviews with senior family office executives to provide quotations and case studies with personal insights that can help family offices to better understand their peers. To make the findings as useful and relevant as possible, this report is interactive, with the option to scroll through the findings by region and size (AUM above and below US$1 billion).

We hope these insights prove useful in shaping cybersecurity planning for your family office, and we would like to offer a heartfelt thank you to all participants who generously shared their time and perspectives.

Figure 1: Participating family office regional headquarters' locations

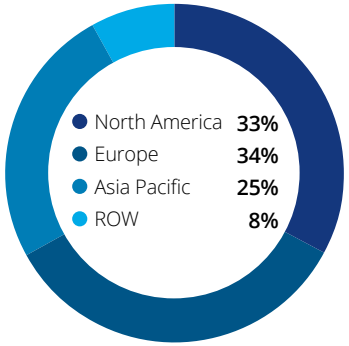
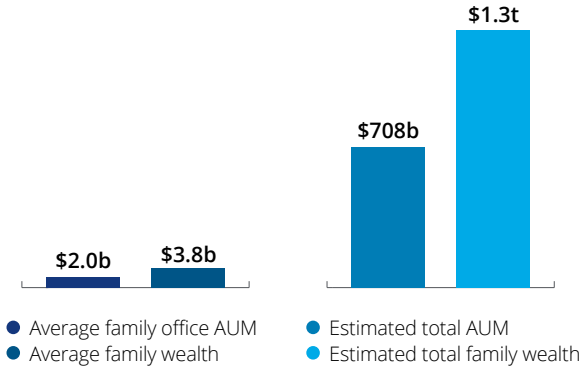


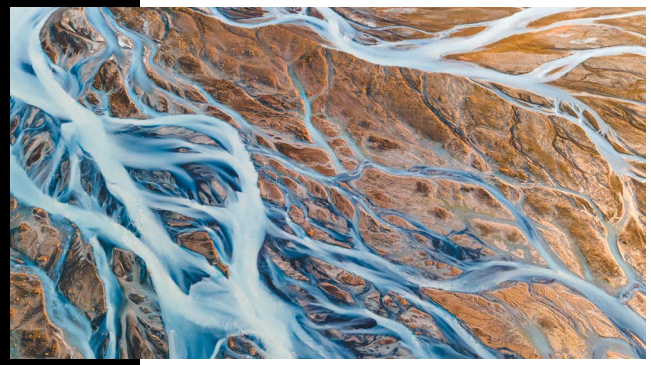
Figure 2: Respondents' family office AUM and family wealth

Click on each button to view the data

Global | North America | Europe | Asia Pacific | ROW

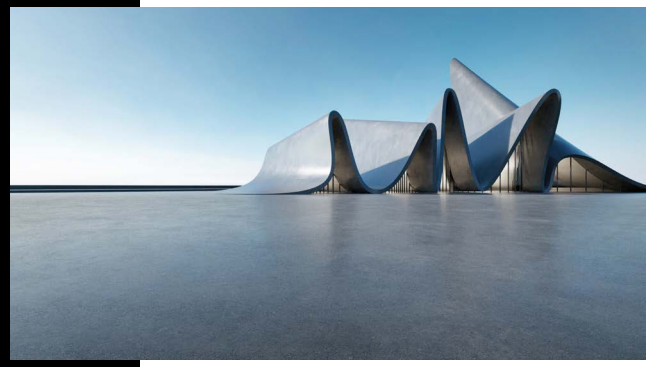


Key takeaways



1 Cyberattacks have become commonplace

A notable 43% of family offices globally have experienced a cyberattack over the last 12-24 months, with 25% experiencing three or more attacks. Those in North America are the most likely to report being attacked (at 57% versus 41% in Europe and 24% in Asia Pacific), along with those with AUM over US$1 billion (at 62% versus 38% for those with AUM under US$1 billion).



2 Threats are varied in nature and often linked

While threats come in many forms and are often linked, the most common form of attack is phishing (experienced by a notable 93% of victims), followed by malware (35%), and social engineering (23%).

3 One-third have suffered loss or damage from an attack

Among the family offices which have experienced a cyberattack, a significant one-third globally have suffered some form of loss or damage as a result. The most common consequences are operational damage (including the loss of confidential/sensitive data) and financial loss, as experienced by 20% and 18% of victims, respectively.

Key takeaways

4 Yet many have no cybersecurity plan in place

Despite the high prevalence of attacks, nearly one-third (31%) of family offices do not have a cyber incident response plan in place. Another 43% say they have a plan, but it "could be better," while merely a quarter (26%) claim to have a "robust" plan.

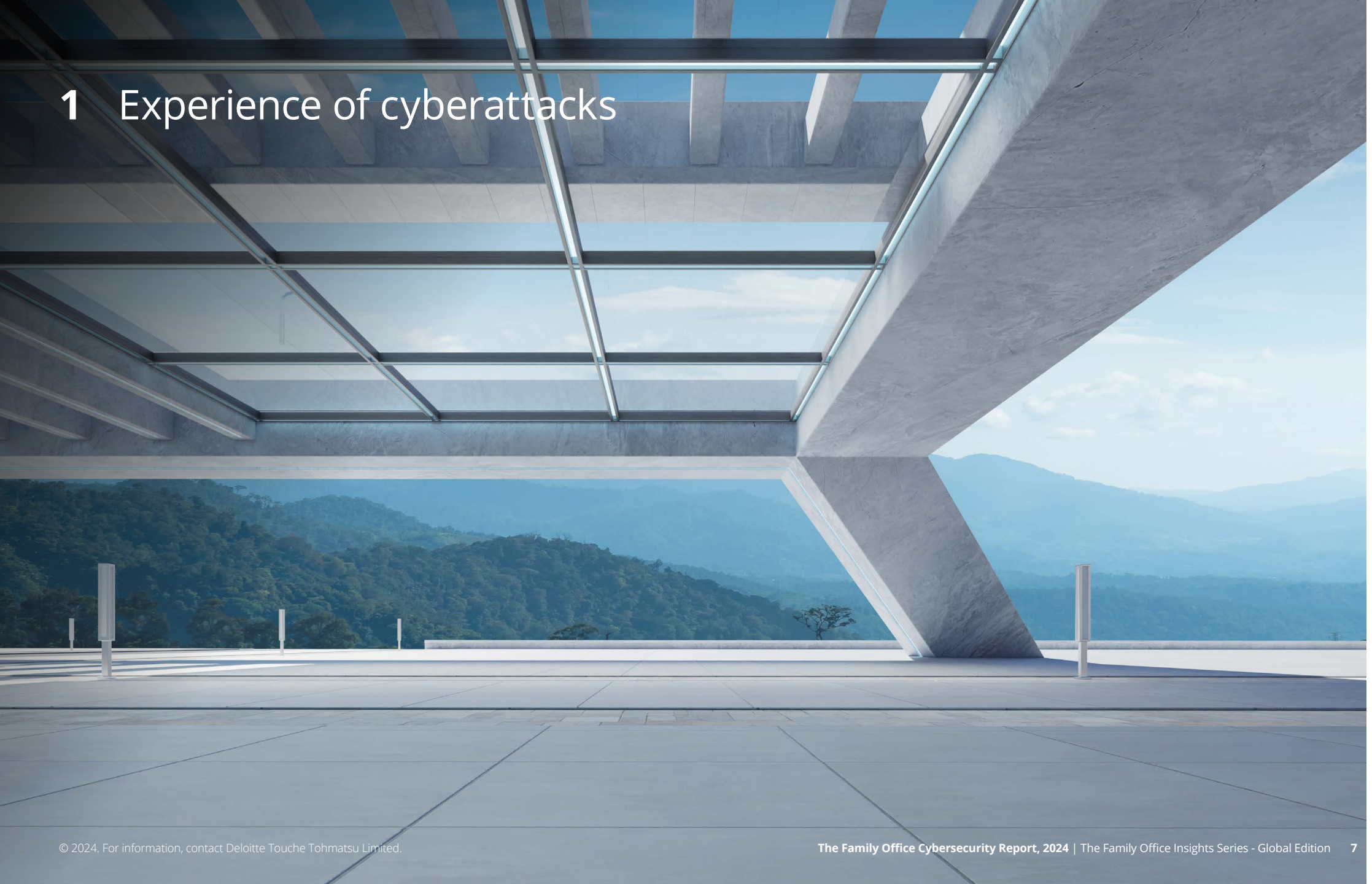
5 Many of the current plans are lacking, leaving family offices open to risk

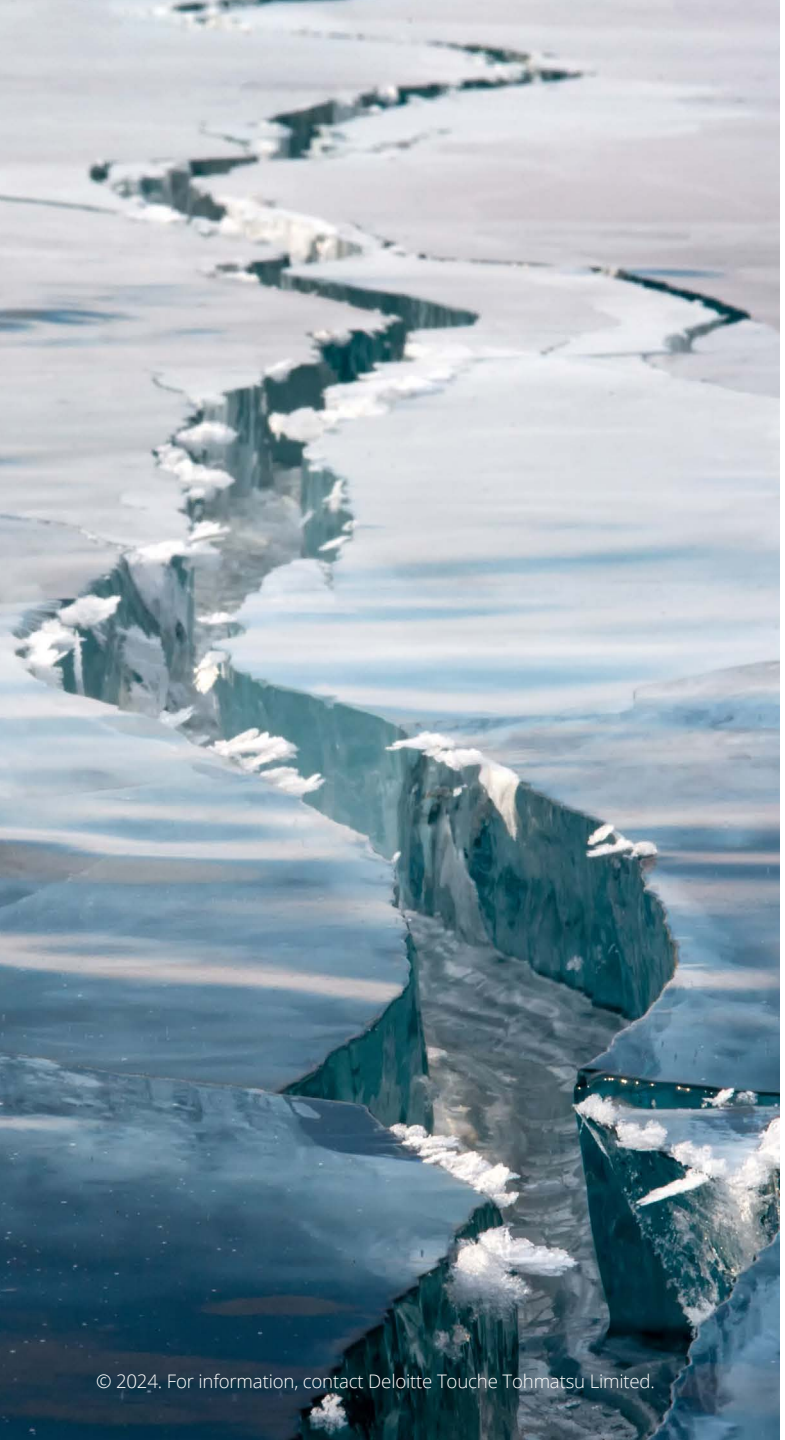
At present, most family offices offer some basic security measures, such as strong passwords/multi-factor authentication (MFA) (85%) and data backups (72%). Fewer offices offer other basic measures, such as cybersecurity staff training (58%) and maturity assessments (34%). Moreover, many offices have not progressed on to more advanced protections that would make them better prepared: 50% do not have a disaster recovery plan, 63% do not have cybersecurity insurance, 68% have not adopted 'know your vendor' protocols, etc.

6 As a result, cybersecurity planning has become a top priority for some family offices this year, but not for enough

Given these security weaknesses, over one in five family offices (22%) have ranked cybersecurity as a top risk to their organization this year. Thus, 15% assert that strengthening cybersecurity is a core priority in 2024, a notable proportion, but one that needs even further visibility given the risks at stake.

1 Experience of cyberattacks





1 Experience of cyberattacks

- A notable 43% of family offices globally have experienced a cyberattack over the last 12-24 months, with 25% experiencing three or more attacks. Those in North America are the most likely to report being attacked (at 57% versus 41% in Europe and 24% in Asia Pacific), along with those with AUM over US$1 billion (at 62% versus 38% for those with AUM under US$1 billion).
- Among the family offices which have experienced a cyberattack, a significant one-third globally have suffered some form of loss or damage as a result. The most common negative consequences are operational damage (including a loss of confidential/sensitive data) and financial loss, as experienced by 20% and 18% of victims, respectively.

Nearly half of family offices have experienced a cyberattack in the past 12-24 months

43% of family offices globally are aware of experiencing a cyberattack within the past 12-24 months (figure 3). This compares with just 30% which reported being attacked in 2021[1], reflecting the rapidly increasing number of cyberattacks worldwide.[2]

In line with the results of a 2023 data breach report from Verizon[3], family offices in North America are far more likely to report being attacked than in other regions (at 57% versus 41% in Europe and 24% in Asia Pacific). North America might be the most-targeted region for cybercriminals because of the complex digital landscapes in the United States and Canada, as well as their relative wealth and influence.

Offices with AUM over US$1 billion are also far more likely to have experienced an attack than those with AUM under US$1 billion, at 62% versus 38%, respectively. They are also more likely to report frequent attacks, with nearly half (46%) saying that they have experienced three or more attacks, compared to just 15% for smaller family offices.

This is likely due to cybercriminals' attraction to bigger pools of wealth and perhaps because larger offices with more sophisticated infrastructures could be more alert than smaller offices to attacks when they occur. However, although larger offices are more likely to report attacks, offices with less mature infrastructures are often more vulnerable to attacks as they tend to have fewer security measures in place.[4] Moreover, should the larger offices be successful at thwarting attacks, this could incentivize cybercriminals to refocus their efforts on smaller, less sophisticated offices.

The frequency of cyberattacks, whether successful or not, may also be higher than the survey results indicate. The family offices which have said they do not know of any attacks may have experienced them but could be unaware that they happened, as individuals are much more likely to be aware of an attack that has successfully resulted in identifiable loss or damage than those that have occurred but remain undetected.

> *You will always have someone try to attack you. It is just a matter of how well you respond when it happens, and the controls you have in place that are fending off attacks before you even know they are there.*
>
> **Brett Treadwell,** Chief Financial Officer, RIDA Development Corporation, single family office, United States

1 Experience of cyberattacks

Types of cyberattacks

Phishing and business email compromise (BEC) – A widespread legitimate-looking email scam where a cyber criminal targets an employee to try to get them to transfer funds/release sensitive info/download malware. Smishing is phishing carried out by means of SMS (short message service) and vishing is phishing carried out by means of phone calls or voicemails.

Malware – Malware is "a program that is inserted into a system, usually covertly, with the intention of compromising the confidentiality, integrity, or availability of the victim's data, applications or operating system, or otherwise annoying or disrupting the victim." A common example of malware is ransomware (a type of malware that holds victims' IT systems hostage until monetary demands are met).

Social engineering – Social engineering involves targeting an individual and persuading them to take an unsafe action, such as transferring funds or releasing sensitive information. The most common forms of social engineering are phishing/BEC and pretexting (gaining a victim's trust and manipulating him/her into believing that the cyber criminal is someone they are not).

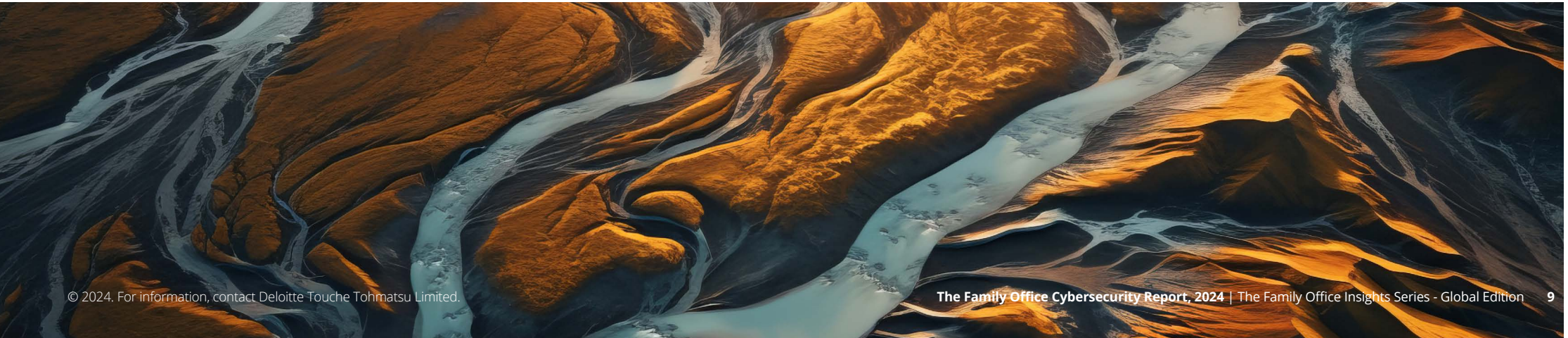
Third-party risk – Where a third party (e.g., a supplier, contractor, or partner) with access to an organization's system or files, damages or harms the office. This can be intentional (the result of a bad actor) or unintentional (the result of an attack on the third party that also impacts the organization).

Insider threat – When an employee intentionally accesses confidential information. This might occur in the form of data manipulation, theft, leaking, and other threats.

Figure 3: Whether the family office has experienced a cyberattack within the past 12-24 months

Click on each button to view the data

Global | North America | Europe | Asia Pacific | ROW | AUM <$1B | AUM $1B+



1 Experience of cyberattacks

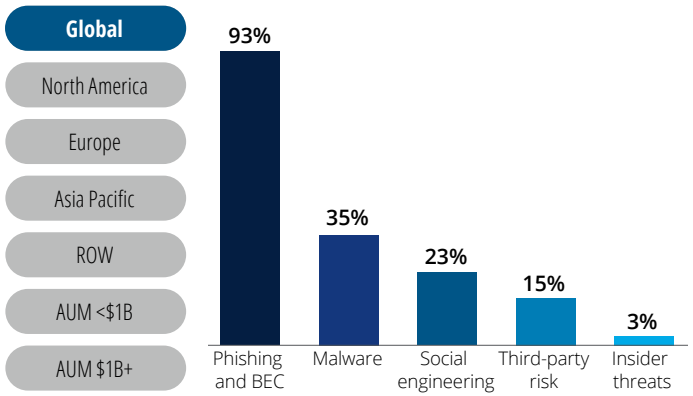
Phishing and malware are the most common forms of attack

The types of cyberattacks experienced by family offices are the same as those suffered by other organizations and, in many cases, by individuals. Nearly all the family offices which claim to have been attacked said that they have received phishing emails (93%), while over one-third (35%) have experienced a malware attack, nearly a quarter a social engineering attack (23%), and 15% have been exposed to third-party risk (figure 4).

It is important to highlight that threats are often linked, such that the goal of phishing may be to install malware, and a technique used to phish for information is social engineering. In turn, as it is harder to detect and thus thwart certain forms of attack, this necessitates the need for staff training, particularly as most attackers just need to exploit one weakness to achieve success.

Figure 4: Types of cyberattacks family offices have experienced

Click on each button to view the data

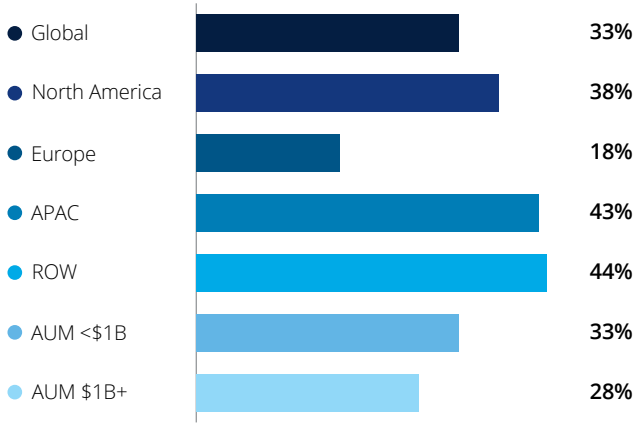


One-third of family offices which have experienced a cyberattack have suffered loss or damage

Among the family offices which have experienced a cyberattack, a significant one-third globally have suffered some form of loss or damage as a result. In Asia Pacific, where fewer cybersecurity defense measures are reportedly put in place than in North America and Europe (figure 10), this proportion rises to 43% (figure 5).

Importantly, despite larger offices (with AUM over US$1 billion) being far more likely to report being attacked than smaller offices (with AUM under US$1 billion) at 62% versus 38%, fewer larger offices have reportedly suffered loss or damage from an attack at 28% versus 33%. This suggests that the smaller offices are less prepared and able than their larger counterparts to ward off attacks.

Figure 5: Proportion of family offices which have suffered loss or damage as a result of a cyberattack



Examples of damage/loss as a result of an attack

- **Financial** – Financial losses can arise on multiple fronts. For example, there can be direct losses from making payments to an attacker in the form of a ransom payment to recover access to one's system/files. These types of attacks can also lead to additional financial losses from operational downtime that directly impact a family office's ability to conduct business and serve the family. Additionally, when attacks are public knowledge, there can be a financial risk to their reputation and brand. It can also be the case where an attacker gains access to a system, lies dormant for a period, and then initiates fraudulent payments, impersonating real people or bypassing security controls.
- **Operational** – A cyberattack may also result in operational disruptions through a loss of confidential data, a negative impact on employee morale (and retention rates), or a change in leadership at the office. For example, malware attacks may succeed in shutting down a victim's IT system, resulting in a halt to operations and possibly a loss of revenue.
- **Reputational** – Attacks could lead to reputational damage, such as negative media coverage, which could make third parties (such as potential lenders, investment managers, or other families) more reluctant to work with families/family offices.

1 Experience of cyberattacks

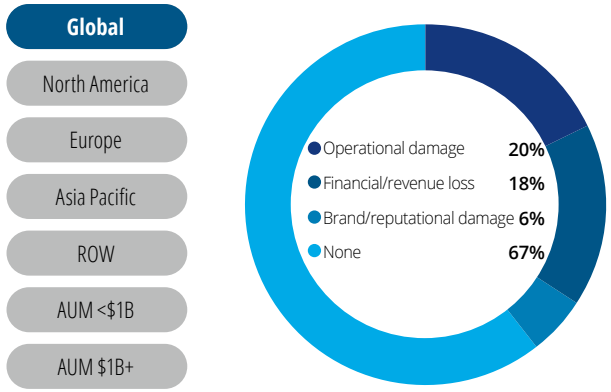
The loss of confidential information and funds are the most common forms of damage

Figure 6 looks at the types of loss or damage those who were attacked have suffered. Here we can see that 20% of those attacked suffered operational damage (including the loss of confidential or sensitive information), 18% experienced financial loss, and 6% brand or reputational damage.

Given that financial, operational, and reputational risks are interrelated, it is important for family offices to assess their points of operational vulnerability, which can lead to data vulnerability, system downtime, and other negative consequences, as this can help mitigate other financial and reputational risks.

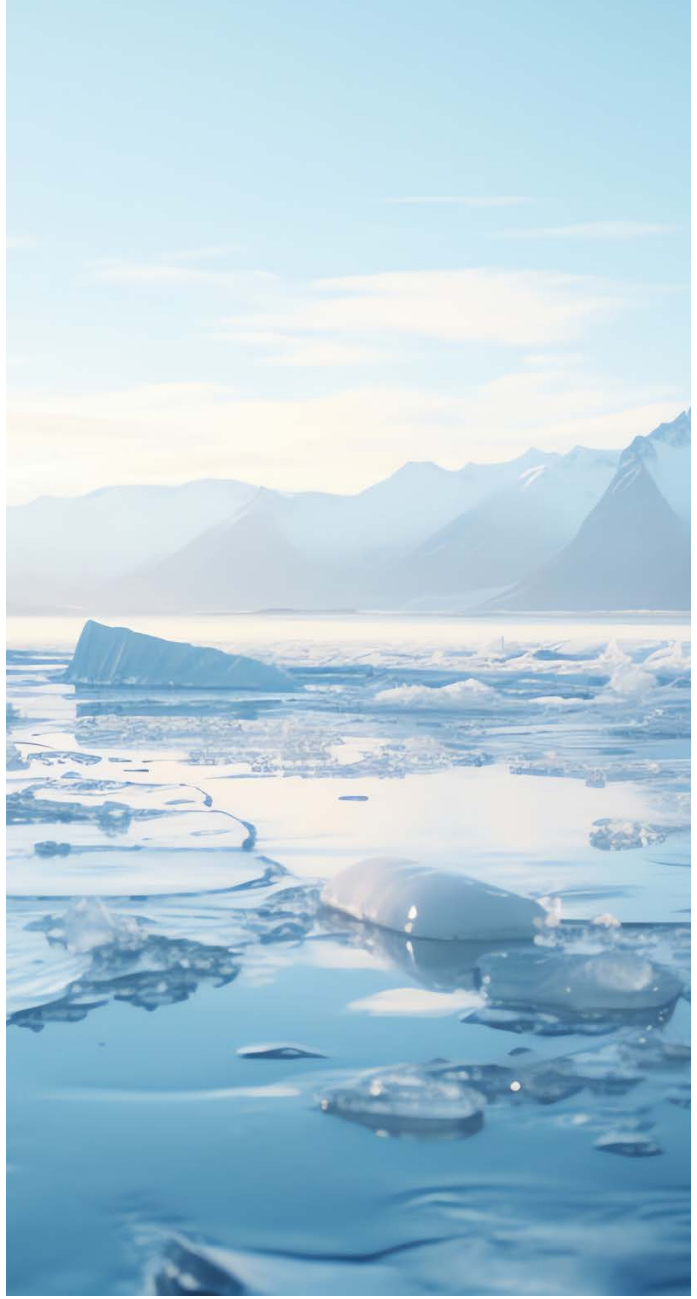
Figure 6: The negative consequences suffered by those which have experienced a cyberattack

Click on each button to view the data



> *There was a breach; someone got into our system. When it was found, all the measures on earth were thrown at it. We used to operate on a server, and a staff member found a draft email from a hacker in a client's account. We shut the system down and we are now serverless, so they cannot do that again. Thankfully, the hacker was stopped before any direct damage was caused. But it created a scare, and that resulted in reputational risk to the family office, as our clients were concerned as we needed to lock down their data.*
> **Director,** single family office, United States

> *The largest amount of money that anybody has stolen from us is US$1,500 in a gift card scheme. A colleague received an email that she thought was from her boss, telling her to send gift cards to a post office box number. Of course, the whole thing was a fraud, but because her boss was traveling at the time and she could not get in touch with him, she unfortunately complied. We have put training procedures in place to help staff members recognize ploys like these.*
> **Chief financial officer,** single family office, United States



2 Cybersecurity strategies

2 Cybersecurity strategies

- Despite the high prevalence of cyberattacks, nearly one-third (31%) of family offices do not have a cyber incident response plan in place. Another 43% say they have a plan, but it "could be better," while merely a quarter (26%) claim to have a "robust" plan.
- To safeguard themselves, most family offices offer some basic security measures, such as strong passwords/multi-factor authentication (85%) and data backups (72%). Fewer offices offer other basic measures, such as cybersecurity staff training (58%) and maturity assessments (34%). Moreover, many offices have not progressed on to more advanced protections that would make them better prepared: 50% do not have a disaster recovery plan, 63% do not have cybersecurity insurance, 68% have not adopted 'know your vendor' protocols, etc.

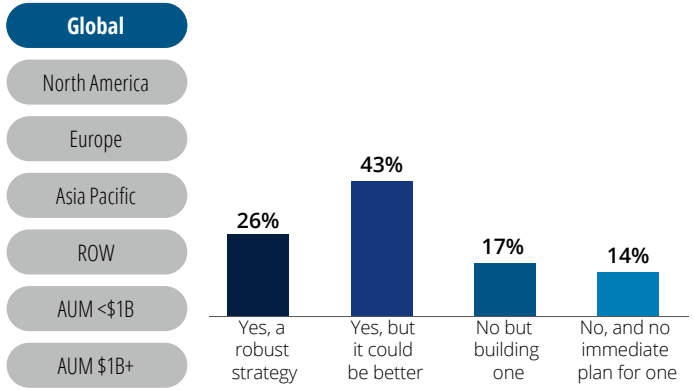
A third are without a cybersecurity strategy in place

Only 26% of family offices globally claim to have a "robust" cybersecurity strategy in place "that has never failed them," with larger offices (AUM over US$1 billion) being more inclined than smaller offices (AUM under US$1 billion) to have a robust strategy (37% versus 18%) (figure 7).

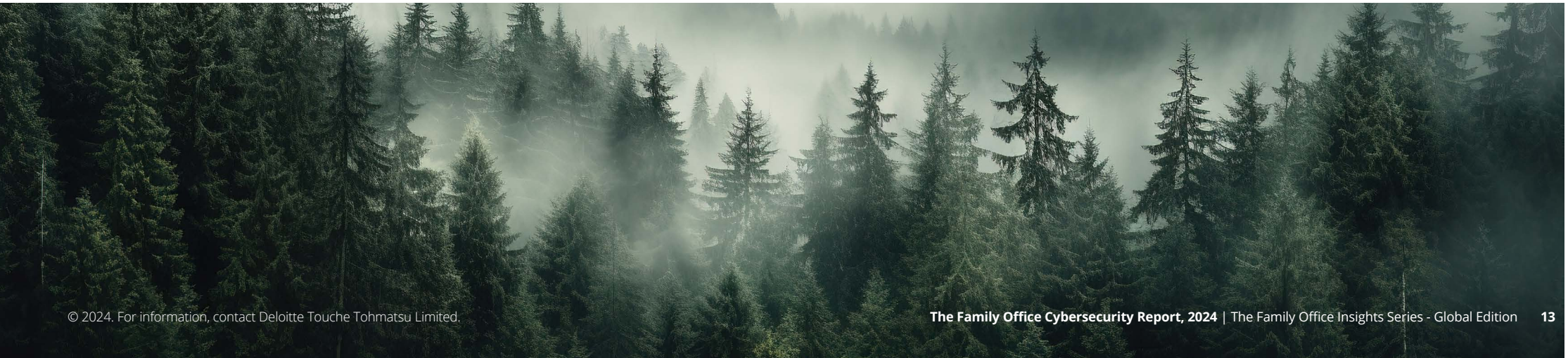
However, 43% of offices with a strategy say that it could be better, while 31% have no strategy at all, with nearly half of these having no immediate plans to get one.

Figure 7: Whether the family office has a cybersecurity strategy in place

Click on each button to view the data



> *Cybersecurity is a big risk. Many people do not react to cyber threats until they have been attacked. A lot of family offices have now been hit and it has made them reactive. Typically, cyber criminals go after the low-hanging fruit, so the less you do, the more likely you will be a target. The more difficult you make it for hackers, the easier it will be to avoid potential problems. Some people do not want to spend money on cybersecurity because you pay all this money and the best thing that can happen is nothing at all. But, if you do not spend the money and something does happen, you can experience a huge loss. It is like buying insurance, it is a negatively skewed investment, but it is one you should not avoid.*
>
> **Chief executive officer/chief investment officer**, single family office, United States



2 Cybersecurity strategies

Most of those with a strategy have it reviewed at least once a year

Given the continually changing nature of cyber threats, it is prudent to review and update an organization's cybersecurity strategy frequently. About half (49%) of family offices with a strategy reportedly review it once a year, and 30% review theirs more frequently than this (figure 8). However, only half (51%) of those surveyed had actually carried out a cybersecurity risk maturity assessment in the past 12 months (figure 9).

> *I want to test our cybersecurity by organizing a planned attack on our systems to determine the vulnerabilities and put the needed safeguards in place to prevent an actual security breach. This is the only way we can find out if we are actually safe.*
> **Chief executive officer**,
> single family office, Belgium

Figure 8: Frequency of updating the family office's cybersecurity strategy

Click on each button to view the data

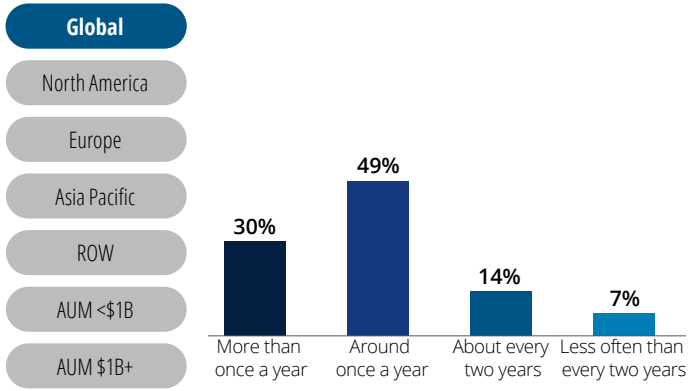
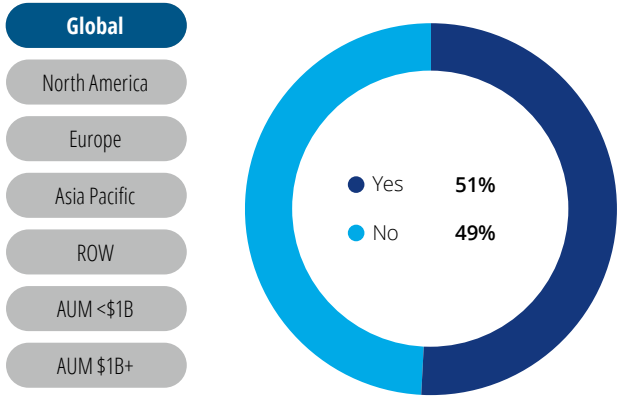


Figure 9: Whether the family office has completed a cybersecurity risk maturity assessment within the past year

Click on each button to view the data



Most family offices employ basic measures to protect themselves but not advanced measures

Most family offices—but by no means all of them—use some well-established "basic" measures for protection against cyberattacks. The most common measures they employ are strong passwords and MFA (85%), and regular software patching/updates (84%). Fewer offices offer other basic measures: for instance, merely 58% offer their staff cybersecurity training, which is a simple, yet effective tool an organization can use to fend off attacks, and just 34% conduct cybersecurity maturity assessments, which review an organization's readiness to prevent, detect, contain, and respond to cyber threats. In general, most of the basic measures noted in figure 10 are used more by family offices in North America than by those in other regions and more by family offices with AUM over US$1 billion than by those with AUM under US$1 billion.

It is even less common for offices to have progressed to more advanced protections. For instance, 50% of offices do not have a disaster recovery plan, which can significantly mitigate the impact of a cyberattack. 63% do not have cybersecurity insurance, and 68% have not adopted 'know your vendor' protocols.

Given the significant rise in attacks, and the notable rate of success cybercriminals have had within the family office arena, there is considerably more that they can do to protect themselves both now and into the future. For instance, as phishing is the most pervasive form of attack among family offices (experienced by 93% of victims), two immediate steps they can take to mitigate this risk are to provide their executives with cybersecurity training and conduct a cybersecurity maturity assessment to judge their ability to fend off attacks.

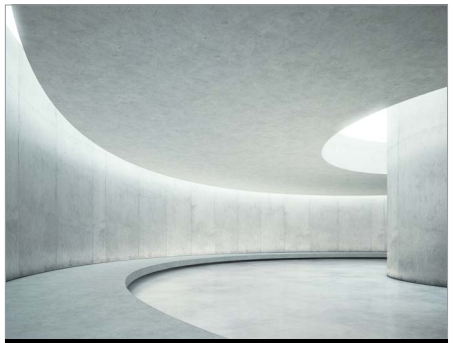
> *Our main cybersecurity concern was to protect our accounting and banking systems. We have moved to multi-factor authentication for the majority of our banking applications and functions. I used to think that it was too much and slowed me down, but now that I have experienced some fraud attempts, I realize that it is worth it.*
> **Chief financial officer**, single family office, United States

> *We have reasonably good cybersecurity systems in place. We have cloud-based security on our machines, which are connected and managed by third-party vendors. Another key focus area for us is reputation management. We use a digital privacy solution provider that protects the personal devices of our leaders. This service safeguards against attacks on their personal accounts or a broader breach into the business or family office while keeping their personal identifying information private.*
> **Chief operating officer**, single family office, United States

2 Cybersecurity strategies

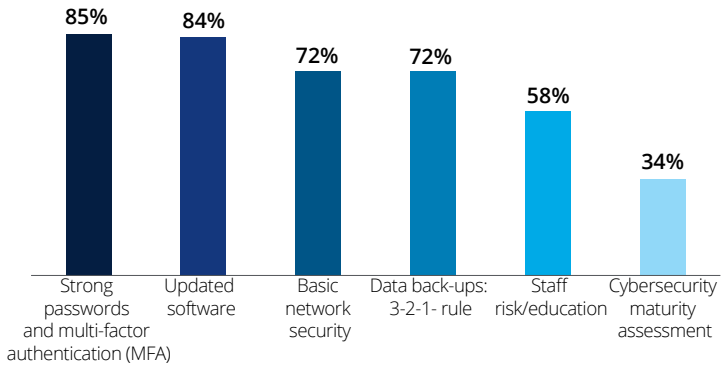
Figure 10: Which cybersecurity measures family offices currently undertake:

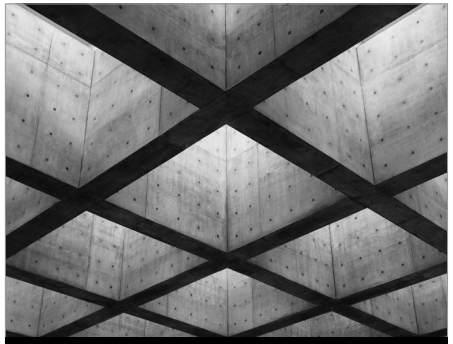
Click on each button to view the data



Basic measures

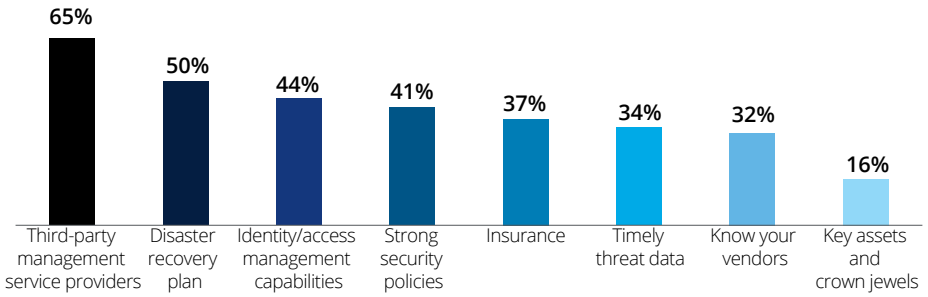
Global | North America | Europe | Asia Pacific | ROW | AUM <$1B | AUM $1B+





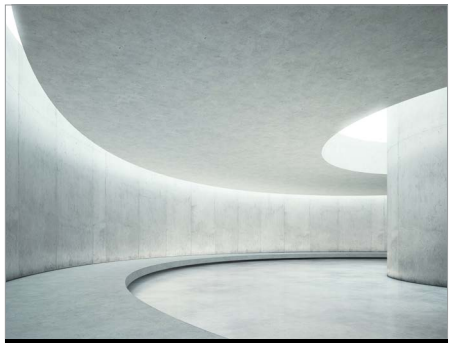
Advanced measures

Global | North America | Europe | Asia Pacific | ROW | AUM <$1B | AUM $1B+



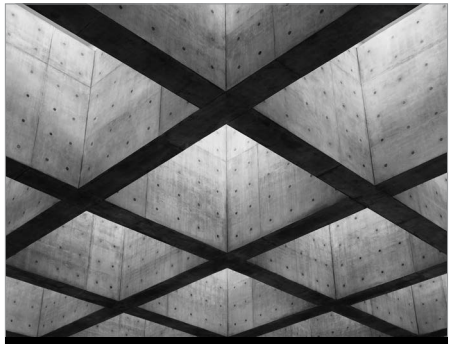
2 Cybersecurity strategies

Explanation



Basic measures

- **Strong passwords and multi-factor authentication (MFA):** Two or more pieces of information are needed to access important websites or applications.
- **Updated software:** Installation of software updates, including antivirus tools, as soon as they become available and keeping an inventory of computers, phones, and other devices to ensure they have updated antivirus/firewall software.
- **Basic network security measures:** Use a virtual private network (VPN) to access the office's network, and a connected device policy for the use of public Wi-Fi/home routers.
- **The 3-2-1 data back-up rule:** Ensure three copies of data are kept on two devices, with one copy held offsite.
- **Focus on staff risk and education:** Background checks on employees and contractors to limit insider threat risk. Educating staff about cybersecurity risks, what to look out for, and how to prepare for a cyber incident.
- **Cyber risk maturity assessment:** Assessments conducted to evaluate the current state or level of cyber maturity and risk in the organization's environment from a people, process, and technology perspective.



Advanced measures

- **Third-party management service providers:** Third-party support to manage and operate cybersecurity processes, controls, vendors, and operating models through a shared responsibility model.
- **Disaster recovery plan:** A plan in place for how the office would sustain operations during an attack and resume normal operations after disruption caused by a cyberattack.
- **Identity and access management capabilities:** Single sign-on, multi-factor authentication, privilege access management with accompanying controls related to who should (and should not) have access to certain data and information.
- **Strong security policies:** Policies and procedures related to day-to-day business operations security such as social media, payments, etc. and a defined approach to monitor and respond to potential threats.
- **Insurance coverage:** Insurance policy offering financial protection should the worst-case scenario materialize. Many providers offer cyber insurance for businesses.
- **Timely threat data**: An internal capability or a commissioned service to monitor online open and closed sources to identify early warnings of potential threats to your business.
- **Know your vendors:** Review your vendors' security, for example requesting security audit reports before contracts are signed.
- **Key assets and crown jewels identification:** Identification of the key assets, intellectual property or trade secrets, sensitive customer information, and other critical information that is most important to the organization and should be protected.

2 Cybersecurity strategies

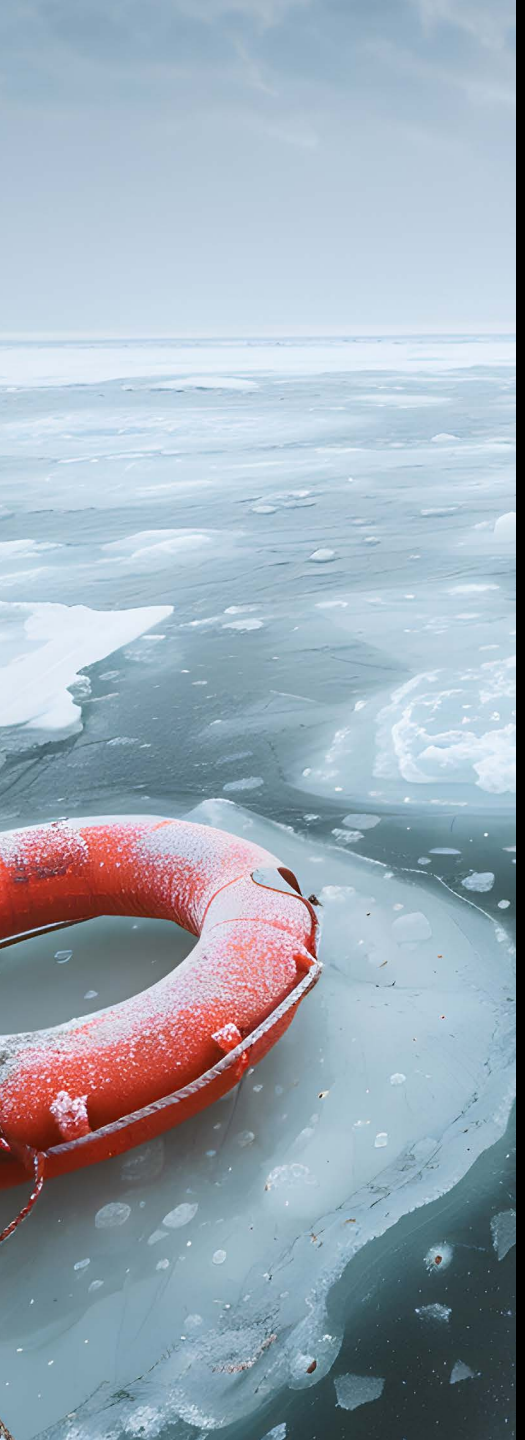
Most utilize a chief information officer/chief information security officer

As an indication of the importance attached to data security, four-fifths of offices either employ a chief information officer/ chief information security officer (36%) or outsource this function (44%) (figure 11). Only 17% of respondents globally assign this responsibility to a member of the C-suite, such as the chief operating officer.

Figure 11: Whether the family office has an in-house chief information officer (CIO) or chief information security officer (CISO), or if it outsources this work

Click on each button to view the data

Global | North America | Europe | Asia Pacific | ROW | AUM <$1B | AUM $1B+



Taking risk seriously: How one of the world's most prominent family offices protects the family's assets and reputation

Cybersecurity and reputation management are two areas the CEO and CFO of one of the world's largest family offices take very seriously, particularly given the universal recognizability of the family. In conversation, they describe a cyberattack their family office faced, and what safeguards they have put in place from both a cybersecurity and reputational management perspective.

What experience does your family office have with cyberattacks?

CFO: "Cyberattacks happen all the time, but we have not had an attack that has been successful."

The CEO added: "In one attack, the level of sophistication was amazing. My assistant got an email from someone who knew I was speaking at a conference. The email was tailored to her as if it were from the event holders. Something seemed wrong, so she had our security team examine the email and they confirmed it was malware. Thankfully, she did not open the attachment."

What kind of cybersecurity protocols do you have in place?

CFO: "We are up to date on our security protocols, and we train our staff members not to click on suspicious links or download data unless it comes from a trusted source. We use an external team and an outside consultant to manage our cybersecurity. We also have a business continuity plan and a risk committee where we discuss risks like these and how to mitigate them."

The CEO added: "The risk committee has four or five members, including outside experts. It ensures that we look at the various risks we face, and ranks them according to how probable and impactful they are, and which ones we need to get in front of. It is a constant, ongoing discussion.

We are really big on risk management. Everyone uses a virtual private network (VPN), multi-factor authentication, a password manager [which alerts people to password breaches], and company-controlled devices. Our phones and computers are managed by the family office. When we travel, we do not use public wireless networks; instead, we use our phones as hotspots. We also instruct third parties twice a year to simulate attacks to test our systems. So, we go pretty far protection-wise."

Has it helped to orchestrate simulated attacks?

CEO: "Yes, it has, as it shows you that human beings are human beings, and they will click on corrupt files they think are safe. It is better to have them make these errors in training than with a real attacker."

Do you have any tips you would like to share with other family offices?

CEO: "The main tip is do not rely on yourself when it comes to cybersecurity. Rely on a third-party expert to check your systems—and get your systems regularly tested."

How do you manage reputational risk?

CFO: "We have security employees who do daily monitoring of the internet and social media and look out for the family's reputational interests."

The CEO added: "I think we manage reputational risk well. We pay attention to what is being said, and we get in front of things if we think there is going to be an issue given that the person we work for is in the public eye. At the end of the day, it is the reputation of the family we are concerned about. I have almost no impact on how they conduct themselves, but we can impact how other people write about them or correct the record if they are saying things that are inaccurate."

3 Strength of safeguards against cyber attack

3 Strength of safeguards against cyber attack

- About half (49%) of family offices say their cybersecurity measures offer protection to a large or very large extent against cyberattacks. This degree of confidence is more prevalent among larger family offices (AUM over US$1 billion) at 70% than in smaller ones (with AUM under US$1 billion) at 37%.
- One in five (22%) family offices globally see cybersecurity as a top risk in 2024, while 15% say that tackling cyber threats is a top strategic priority this year.

Half lack confidence in their cybersecurity program

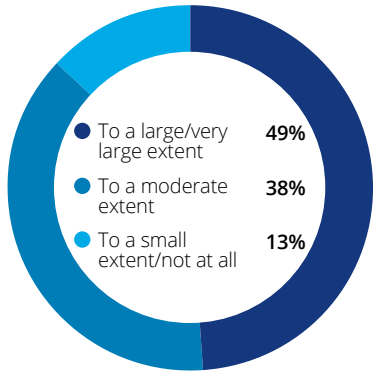
Roughly half of family offices globally (49%) believe that their measures to safeguard against cyberattacks are either strong or very strong, while the other half (51%) feel that they are only "moderately" effective (38%) or simply ineffective (13%) (figure 12). Lack of confidence in cybersecurity measures is highest among those with AUM below US$1 billion (with 64% moderately or less confident) and lowest among those with AUM over US$1 billion (30%).

However, confidence in cybersecurity measures could be based on two different viewpoints. Family offices with robust security measures in place might be confident that they are effective, while others who might not have robust measures in place could also be confident in their effectiveness because they perceive the risk of cyber threats to be low. In turn, such factors should be taken into consideration for perception-based results.

Figure 12: The extent family offices feel they are adequately prepared to safeguard themselves from a cyberattack

Click on each button to view the data

Global | North America | Europe | Asia Pacific | ROW | AUM <$1B | AUM $1B+



3 Strength of safeguards against cyber attack

Over one in five perceive cybersecurity to be a top risk in 2024, while 15% are making cyber protection a core strategic priority

When asked about the main risks they face in 2024, 22% of family offices identified cybersecurity as a top risk (figure 13). This perception of risk is higher for offices in North America (30%) and for those with AUM over US$1 billion (29%) than for those in Europe (19%) and Asia Pacific (18%), or those with AUM under US$1 billion (20%).

In light of these perceptions of risk, 15% of family offices globally (but 25% in North America and 22% of those with AUM over US$1 billion) have made tackling cyber threats a top strategic priority this year. This compares with just 11% of family offices in Europe and 8% in Asia Pacific (figure 14).

With these results in mind, it seems that awareness of cybersecurity risk could be stronger among those in North America and those with larger AUMs than others. That said, as the number of cyberattacks is increasing worldwide[5], it is important for family offices across all spectrums to view cybersecurity as a critical component of their overall business strategy, technological ambitions, and risk management capabilities.

Figure 13: Proportion of family offices which rated cybersecurity as a top perceived risk to the family office in 2024

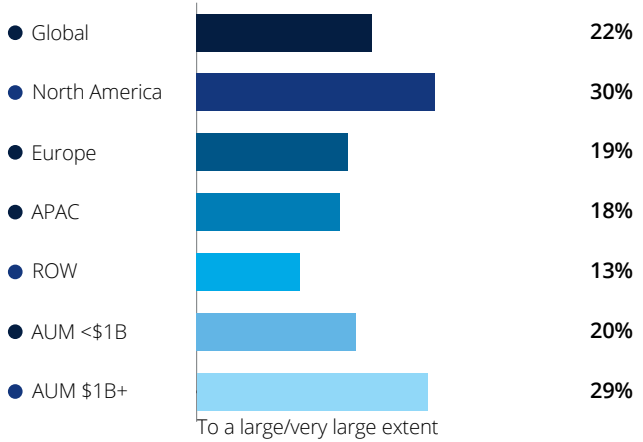
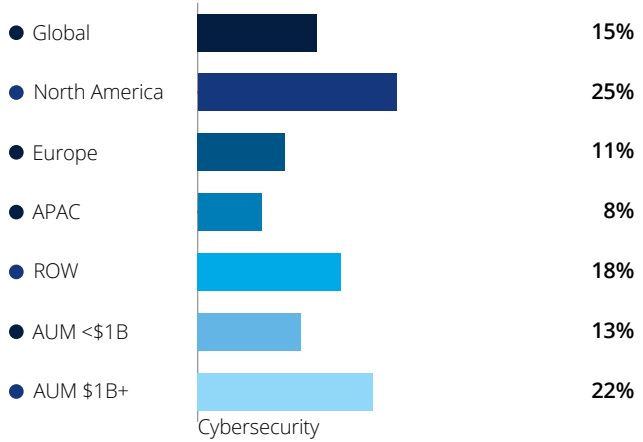
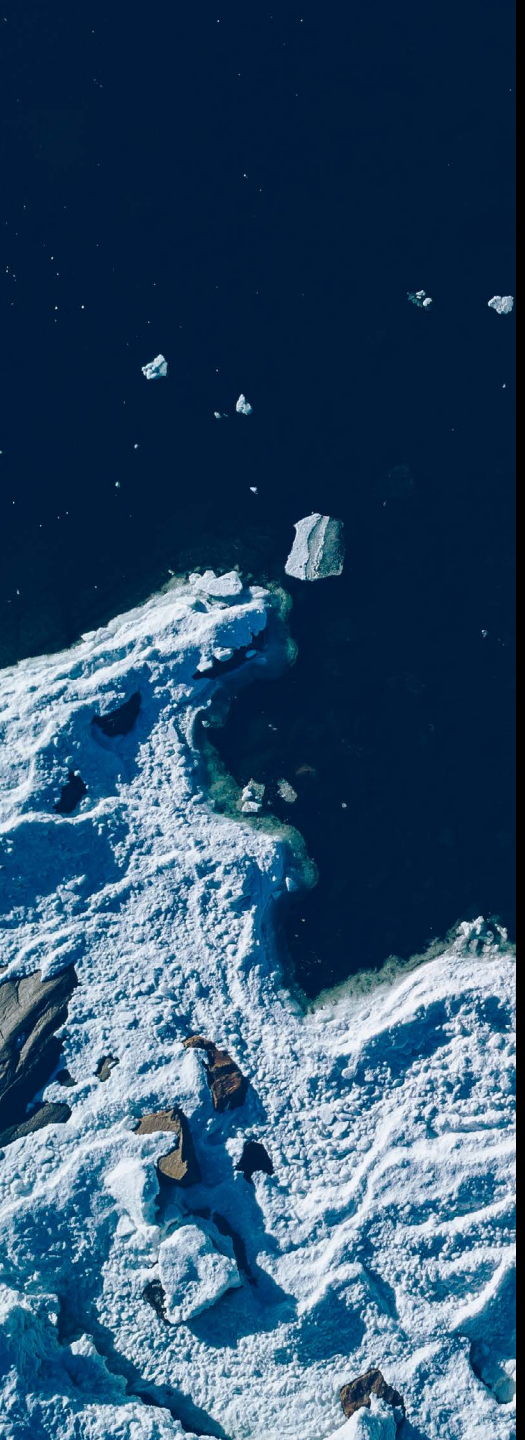


Figure 14: Proportion of family offices which rated cybersecurity as a top strategic priority in 2024





“After two attacks, we took a hard look at our cybersecurity strategy”

The CEO of a United States-based family office retells the story of how both he and a family member got hacked. He discusses how they responded to the attacks by upping their cybersecurity defenses and offers tips for other family offices at risk.

Can you outline the cyberattacks you suffered?

“We experienced two cyberattacks in short succession. In the first instance, a family member’s bank account was hacked. Someone tried to transfer money out of the account, but thankfully the bank had controls in place to stop them. We put out alerts across the board once it happened, but we never figured out how they got in.

In the second incident, someone hacked into my account. They tried to replace me at the institution by putting in the contact details of another person. I am the signatory on a lot of our accounts, and someone was able to get into my account and email the back office at our banks and tell them that I changed my address and phone number. It was really alarming. From a risk perspective, cybersecurity is the thing I am most worried about. The threat is everywhere.”

What were the repercussions of these attacks?

“Thankfully, we incurred no damage from the attacks, as the banks caught them as they were happening. I was impressed with how they managed to stay on top of things. They immediately notified us of suspicious activity both times, and we confirmed that we did not authorize the activities. However, the executive team and I felt very vulnerable because of the attempted breach. I needed to separate my emotions from my job and focus on reducing the risks going forward. We have since put tighter controls in place and have instituted alerts across all our accounts.”

Did your family office change its approach to cybersecurity because of the attacks?

“The first thing we did after the attacks was hire an outside expert to come in and take a hard look at our internal processes and controls. We wanted to ensure that we are doing everything we can to protect ourselves. We then upgraded our cybersecurity team from an individual IT consultant to an outside firm, as we felt that our office’s activities were getting too complex for one person to stay on top of. It has been a nice upgrade, and we are constantly talking to the firm about how to handle emerging threats.

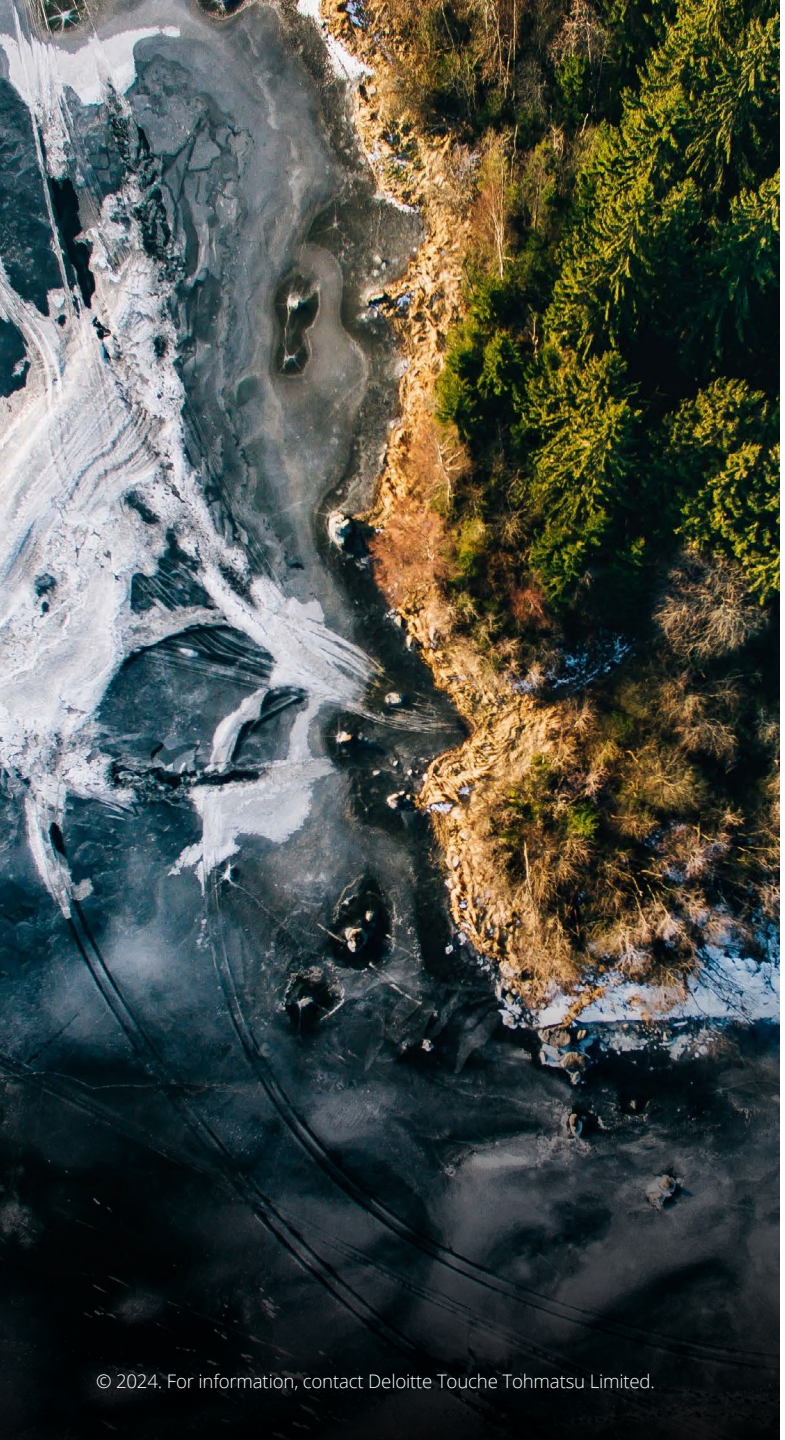
We are putting up as much firewall as we can, so we also provide staff with a lot more training now about phishing and other threats. We have also implemented two-factor authentication and annual reviews and tests of our systems, firewall, and disaster recovery plans. And, thankfully, the family I work for is very low key. They are not in the public eye by design, so that is a risk mitigator.”

Having gone through this experience, what advice do you have for other family offices?

“Having your family office’s internal controls reviewed by an outside institution is very valuable. We do it now every three years. It is extremely important, as family offices are typically small and work in a vacuum. We do not have a big institution behind us, so it is extremely important to have outside help to review your systems and processes.

I go to meetings and join groups to meet other family office executives, but in the end, I still go back to working in a small office. Unless you are one of the rare family offices that has hundreds of staff, you are reliant on a small group of people. You must trust them, but you also must put policies and procedures in place to ensure that you are mitigating every threat you can. Overall, we feel more secure thanks to all that we have done, but you can never feel completely safe because the bad actors are always inventing new ways to attack.”

4 Next steps: Leading cybersecurity practices for family offices



4 Next steps: Leading cybersecurity practices for family offices

Family offices play an essential role in the economy, creating and managing trillions of dollars in wealth for both individuals and institutions. However, this analysis shows that many family offices are highly vulnerable to phishing, malware, ransomware, and other cyberthreats which put them, the families they support, and wider financial networks at risk.

To put a foundation in place to minimize operational, financial, and reputational losses that result from cyberthreats, family offices can consider introducing the basic and advanced actions outlined earlier in this report. In particular, an annual cyber risk assessment, basic training for all employees on phishing/malware risks, and a mature approach to data/information access using multi-factor authentication (at a minimum) or identity and access management (IAM) controls (the preferred approach) is advisable.

For best practice, here are 10 steps family offices can take to safeguard themselves:

1. Have a threat-informed cybersecurity operations program that can detect and respond to threats and incidents. This can be run with the help of a trusted third-party managed services provider.
2. Complete a cybersecurity maturity assessment every one to two years. Consider conducting penetration testing at least once a year by a third-party provider.
3. Implement strong identity and access management (IAM) controls across your organization, giving access to individuals for specific information based on their role or function.
4. Implement a robust third-party risk management program that takes into account cyber risk.
5. Establish a baseline to identify your organization's critical assets, data, and other sensitive information. Identify where it is being stored, evaluate who has access to the data/assets, and implement data protection and data monitoring for those assets. Update legacy servers and other software that is outdated or no longer being maintained by the manufacturer and cannot be patched.
6. Educate/train users about social engineering-based phishing and malware campaigns.
7. Develop a cyber incident response plan and exercise it regularly with key stakeholders.
8. Implement an IT disaster recovery plan that contains procedures for conducting regular data backups that may be used to restore organizational data.
9. Develop a business continuity plan to enable the business to function in the event of loss of technology.
10. Determine risk tolerance and cybersecurity insurance levels needed to mitigate financial risk.

If you would like to learn more about cybersecurity, please click here to read Deloitte's 2023 Global Future of Cyber Survey.

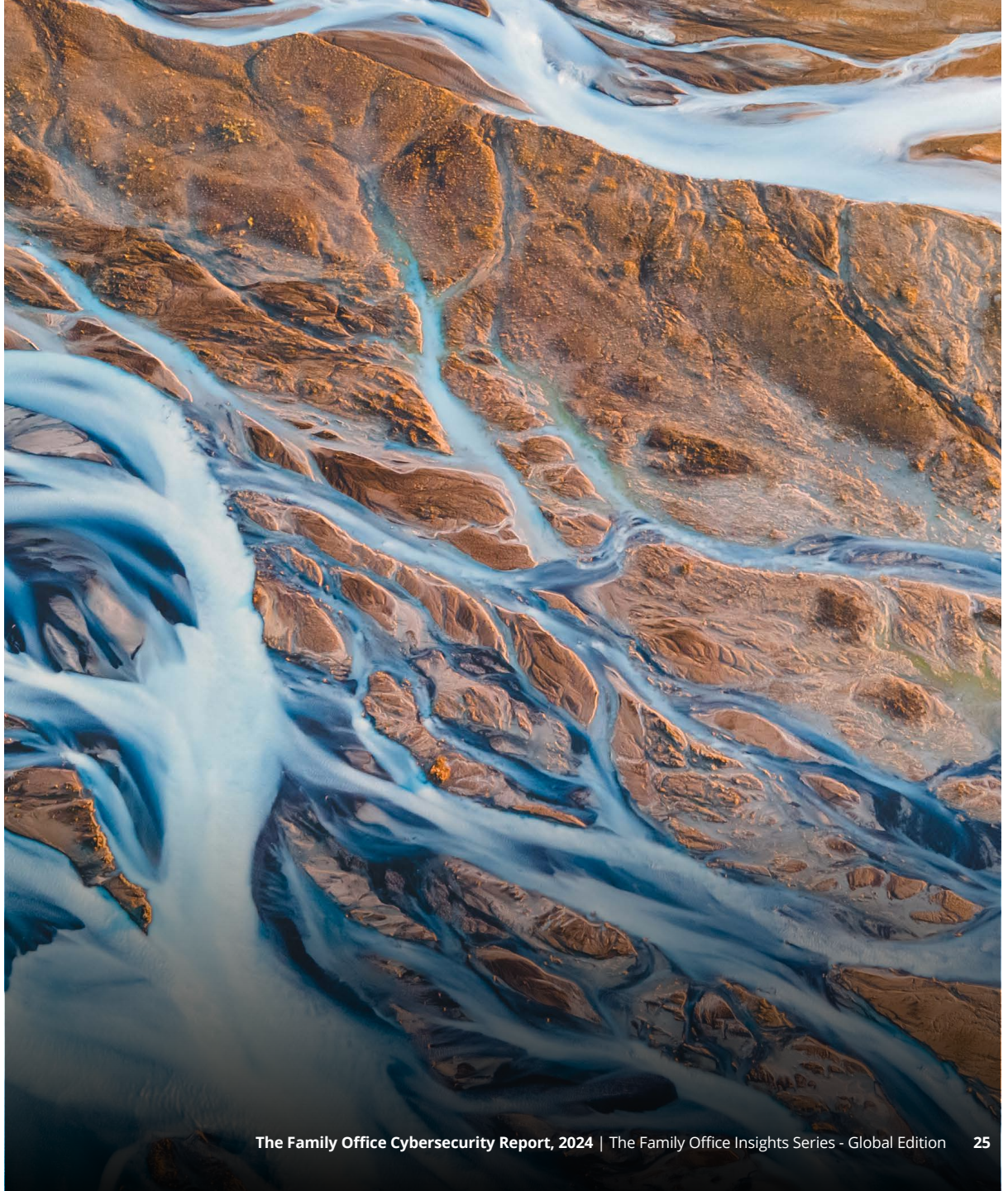
If you need help getting started or have questions about the measures your family office can take to protect itself, please get in touch.

Contact

Dr. Rebecca Gooch
Deloitte Private Global Head of Insights
2 New Street Square, London, EC4A 3BZ, United Kingdom
Direct: +44 20 7303 2660 | Mobile: +44 (0) 7407 859053
rgooch@deloitte.co.uk | www.deloitte.co.uk/deloitteprivate

Nick O'Kelly
EMEA Cyber Incident Response Lead
Partner I Deloitte LLP
1 New Street Square, London EC4A 3HQ
Direct: +44 20 7007 0136 | Mobile: +44 7880 262760
niokelly@deloitte.co.uk | www.deloitte.co.uk/deloitteprivate

Christina Staples
UK Family Office Leader
2 New Street Square, London, EC4A 3BZ, United Kingdom
Direct: +44 20 7007 8273 | Mobile: +44 7771 797475
cstaples@deloitte.co.uk | www.deloitte.co.uk/deloitteprivate



Endnotes

1 Deloitte Private/Campden Wealth, The European Family Office Report, 2021, page 58.

2 Check Point, Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks, 5 January 2023.

3 Verizon, 2023 Data Breach Investigation Report, page 70.

4 The Deloitte 2023 Future of Cyber Survey found that organizations with lower cyber maturity levels experience more significant cyber events, page 12.

5 Check Point, Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks, 5 January 2023.

Deloitte.
Private

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Private is the brand under which firms in the Deloitte network provide services to privately owned entities and high-net-worth individuals.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 457,000 people worldwide make an impact that matters at www.deloitte.com.