MOORE STEPHENS

Cyber Risk Report

Family offices

Cyber Risk Report – Family offices

Contents

Introduction

In recent years there has been a drive to invest in the latest technology. There are a number of reasons for this, for example to provide more timely and meaningful management reporting, support diverse investment portfolios or enable efficient, 'straight through' processing of transactions.

While this investment in technology can bring massive benefits to a modern family office, it also introduces unfamiliar risks, such as cyber security. Cyber threats are those that relate to the loss, removal or amendment of information that resides on, or is processed by, technology. These risks can arise from within and outside an organisation, and from employee error or deliberate action.

The increasing scale of reported data breaches and security failings confirms the extent of the cyber risks that all organisations face. Family offices are no exception, but how well protected are they? Industry reports suggest that the majority of organisations have suffered some kind of information security breach, and our experience of working with family offices indicates that many have suffered in some way.

This report focuses on the cyber risks to look out for and how family offices can, and should, respond to this risk.

Key findings

- Boards are concerned about the threat posed by cyber security issues – but many are not concerned enough.
- Family offices are failing to take sufficient action to ensure suppliers and service providers have adequate cyber security arrangements in place.
- Almost a third of family offices surveyed have no formal information security policies in place.
- Responsibility for cyber security is most likely to rest with IT – but is this the best solution?
- Staff in most family offices need more regular training on cyber risks and information security.

Technology undoubtedly changes the risks faced by a family office, particularly when faced by highly motivated and capable cyber attackers. While it is impossible to eradicate this risk, we hope you find our paper a useful starting point to help you manage it to an acceptable level. Technology adoption seems to be irreversible.

Time to build defences: family offices cyber risk survey results

The increasing number and scale of reported data breaches confirms the extent of the cyber risks that all organisations face. Family offices are no exception, but how well protected are they?

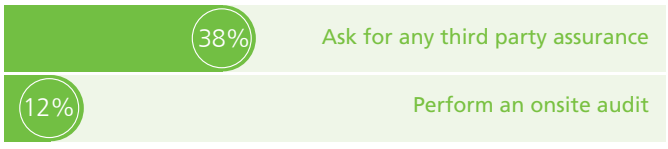
We conducted a recent online survey among family offices. Many respondents' operate globally, in North America, Europe and Asia, and almost a third (31%) have over $1bn in assets under management. They have much to lose from a cyber security or data breach.

Our findings suggest some awareness of the cyber threat, but huge scope for improvement in the actions that family offices could and should take to protect themselves.

Boards are concerned about the threat posed by cyber security issues – but many are not concerned enough.

All survey participants expressed concern about cyber security threats. From one perspective, this is an encouraging result – cyber threats are real and significant and need to be taken seriously. However, a third of respondents (31%) are only 'slightly' concerned, which is worrying. Cyber attacks have been identified as a 'top 10' global risk by the World Economic Forum, so all organisations – family offices included – should view cyber security as a major issue about which they should be very concerned.

Family offices are failing to take sufficient action to ensure suppliers and service providers have adequate cyber security arrangements in place.



Our contact with small organisations, particularly those in the family office sector, has shown that security risk often sits with third parties in the supply chain, rather than directly in-house. It is therefore surprising that only 38% of respondents ask for any third party assurance that service providers have adequate cyber security arrangements in place, and only 12% perform an onsite-audit. The action taken by the highest proportion of respondents – though still less than half – is to lock security requirements into contracts. We would expect more family offices to take at least this step to protect themselves from cyber risks.

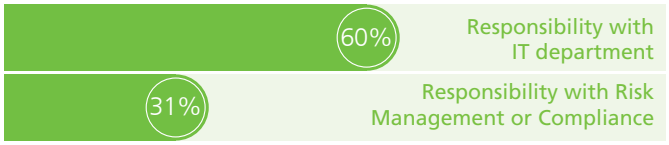
Of respondents who said they performed 'other' actions, some admitted to not doing much, or were currently developing policies, or requested specific information on security from suppliers.

Almost a third of family offices surveyed have no formal information security policies in place.

The adoption of formal information security policies represents a fundamental building block in any entity's defensive wall to counter cyber risks. Among respondents, 71% said their organisation has formal information security policies already in place. This is a positive result, given the limited cyber security and IT skills available to many family offices.

However, the fact that 29% have no formal policies in place is a huge concern. This suggests that within these organisations the nature and extent of the threat posed – and the damage that could be done by a security breach – is not fully understood.

Responsibility for cyber security is most likely to rest with IT – but is this the best solution?



Asked who in the organisation is responsible for cyber security, 60% named their IT department; Risk Management or Compliance held responsibility in 31% of cases. Other functions with responsibility included Operations (17%) and Finance (10%).

The IT department may seem an obvious home for cyber security management, but it is not where responsibility should lie. There can be clear conflicts of interest if the same people are both controlling and managing the cyber risk, both building or commissioning IT security systems and also monitoring them.

This finding provides a further indication that senior managers within family offices do not fully understand the cyber security threat. If they do not fully understand it, how are they to manage it effectively?

Staff in most family offices need more regular training on cyber risks and information security.

38% Staff receiving training only 'infrequently' or not at all

A large proportion (38%) of family offices train their staff or management on the cyber threat and information security only 'infrequently' or not at all. This is a concern because human behaviour is vital for protecting organisations from the cyber risks they face. For example, staff need to know what to do if they click on a dubious web link, or who to speak to if they suspect some other security breach has taken place. Regular training and awareness-raising is necessary to reinforce understanding among all staff of the importance of applying policies and controls.

Family offices generally have a good level of integration between their risk management and cyber security approaches.

21% Some integration

62% Constant integration

Around one in five respondents (21%) report constant integration of cyber risk and overall risk management, while another 62% achieve at least some integration of approaches. This relatively high level of integration activity is to the credit of the organisations concerned, because it can be difficult to achieve. However, this finding seems slightly at odds with less positive earlier responses revealing a lack of formal information security policies and third party assurance on suppliers.

In summary

Cyber attacks can inflict huge damage on organisations whose policies, processes and controls leave them unnecessarily exposed. Our survey indicates that many family offices currently have inadequate defences in place to protect themselves from attack. Those that lack formal information security policies, overlook their supplier risks, fail to train staff and leave cyber security to their IT specialists are encouraged to take urgent action.

Cyber security threats – what actually goes wrong

2016 has brought fresh reminders of how organisations' data can be vulnerable to attack. Every individual and firm must make sure they have taken key steps to protect themselves.

Two headline-grabbing events this year serve as a useful reminder of the threats organisations face, whether from external or internal attack.

SWIFT warning

Earlier this year hackers stole $81m from accounts at Bangladesh Bank within hours. The good news is that the thieves had been aiming to steal $1bn – a typo in one of the falsified money transfer requests scuppered their plan. Nevertheless, $81m is still a lot of money.

The theft is also newsworthy because it was achieved by hacking systems feeding into the SWIFT payments platform connecting banks around the world. Other banks as well as Bangladesh Bank also appear to have been targeted in this way, although the success of any such attacks has not been revealed.

The SWIFT breach provides some clear lessons.

1. Hackers aren't only interested in stealing data or personal banking systems, but are also keen to attack commercial payment systems. SWIFT has indicated that it will be publishing security standards, which all relevant parties should apply.
2. Don't rely on third parties for your security. In the SWIFT attack, systems feeding into the payment platform were breached. It's important to be aware of the depth of technical risks that can be associated with linking to third-party systems and processes.
3. Make sure you have applied all the basic principles of cyber security. Much of the public information on this hack seems to imply that the basic security controls were not in place in this instance.

Email losses

The biggest headlines this year were caused by the news that some 11m documents held by Panama-based law firm Mossack Fonseca has been passed to a German newspaper. The documents, containing potentially compromising information on high profile clients' tax planning, were apparently obtained by a whistleblower breaching the firm's email server.

The experience of Mossack Fonseca also triggers some key points of advice.

1. Make sure you understand what third parties are holding data related to you and your affairs.
2. Be prepared: if such a third party suffered a data breach so that you or your organisation was thrust into the public eye, how would you respond?
3. Don't underestimate the importance of emails. They often contain substantial data, making email systems an attractive prospect for hackers.
4. Many people take a less formal tone when writing emails, but care should be taken. A comment made in jest in a 'private' email could cause substantial problems if taken out of context in a public breach. Email comments may seem passing, but can create an indelible link with the name of an organisation or individual.

Both these issues relate to third parties. In the first case, the issue relates to how the family office interacts with a major third party (SWIFT) and highlights how criminals will look for the point of vulnerability regardless of who is responsible. In this case, passing much of the processing on to third parties does not fully mitigate the risk of fraud. In the second case, the issue is directly involved with the security of data held by third parties.

There are far more types of information security failure that family offices should be wary of, however. Three things we see going wrong, and things family offices should consider, are:

Viruses and malware

We are all familiar with the idea of viruses, and most of us think we have things under control here. This might be complacency or wishful thinking, as malware continues to pose a real threat to most organisations.

Anti-virus software provides some control, but it is very far from perfect – don't assume that just because you have anti-virus software you are protected. Viruses are often contracted by visiting an infected website or opening an unsolicited email attachment. However, don't assume that this is just the actions of a careless user – some of the largest, most commonly used websites in the world have been hacked to deliver viruses, and do you really check every single link you click on? We also see far more sophisticated email 'spam' to entice users to a fake website or to open attachments, so please don' think you are immune.

What will the virus do? This varies, but common examples include:

- open a door for hackers to access your system directly;
- encrypt some of all of your data, and demand a ransom to unlock this;
- record the activity and data on that computer (for example, passwords and credit card numbers) and automatically pass these to someone outside the organisation.

Employees being 'helpful'

We like to think of cyber security threats as being highly technical, difficult to perpetrate and somehow beyond our understanding. In reality, the most common way implementing technology leads to family offices losing control of their data will be through an employee misjudgement or mistake. For example:

- employees emailing sensitive data (holdings, bank account details, personal data) unencrypted means that the email will be sent over a public network without having been encrypted. Anyone able to intercept or copy that email on route will be able to read it all.
- storing data on public cloud services or on personal email. Using public 'cloud' services to share information can be really efficient, but you often have no control over access to or sharing of that data once it's left your systems. It makes little sense to build a highly secure set of internal systems that heavily restrict access to data if your employees are going to use public cloud services to share it.

Securing digital channels is a complex exercise, and one that draws on a range of governance, risk and assurance capabilities as well as in-depth technical and cyber security skills. We introduce the common steps to address these cyber security threats overleaf.

Regardless of the standard you adopt, if any, no one in the family office industry can ignore this complex and growing threat. At the very least, you should:

- educate your senior management and employees on security threats and how to respond to these;
- architect your risk, policy, technology and standards environments to help you ensure your business operates according to your risk appetite;
- assure your process and technology, giving you independent and timely information on your state of information security compliance;
- manage your security operation, making sure you blend education, architecture and assurance in a way that is appropriate to your organisation.

Given the ingenuity of hackers, there's no doubt about the inevitability of future cyber attacks, causing financial, data and reputational loss. Taking action to understand how things actually go wrong – and to plan for how to respond to any such attack – is the only sensible precaution.

Simple solutions to a complex problem

Managing the cyber security risk is an ongoing process, and one that will never completely eradicate your risk of failure. While there are standards that can guide you through this process, the challenge is often not whether to conform to a standard but which one to follow. In this section we introduce the standards and sources of guidance that we prefer to use and summarise the main themes so you can design your programme to fit your organisation and culture.

ISO27001 – Information Security Management

This is, and will remain, the primary standard for security. On first reading, it can appear cumbersome and disproportionate to many organisations. However, when applied by a skilled practitioner the standard can apply as much to a small family office as a multinational financial institution. The heart of the standard suggests that:

- security is a process, not a destination, and that to embed this process you need to (a) plan what you intend to do (b) actually do it (c) check it's working properly, for example through testing, auditing or ongoing monitoring and (d) act appropriately when you find it's not working properly. Then you start the planning cycle again;
- security is far more than technology. Both ISO27001 and its partner guide ISO27002 offer target controls for technology, but also people, management, third party oversight, physical security and risk management. We have found it an extremely useful tool for making sure a security programme is covering the right areas.

'Top 20' Security controls

Both SANS and the UK 'centre for the protection of national infrastructure' (CPNI) maintain a list of 20 controls organisations should have in place to manage the cyber risk. While these tend to be more technical in nature, applying a list of 20 controls can be more straightforward than finding a skilled practitioner to implement ISO standards. While they aren't designed to cover all the same areas, the simplicity of the list offers a great reference point for organisations trying to manage the cyber security risk.

10 steps to cyber security

The UK Government recognised the need for practical guidance to help organisations manage the cyber security risk, and proposed '10 steps' organisations should take to help manage the cyber security risk. It is a useful resource – the Government has also prepared board briefings and implementation packs to support the guidance. The scope ranges from 'information risk management' – so the process of understanding the data you have and how it could be at risk, to more specific technical controls designed to mitigate many of the vulnerabilities that lead to people being hacked (such as firewalls and virus protection).

Source: UK Government

There are many other excellent standards available – every practitioner will have their particular favourite. For family offices just starting their security programme, our summary of the key points is outlined below:

Know your data, who has it and what could go wrong

You can't protect everything. Start your security programme by understanding what data you have, where it is (for example, which system, which third party) and how important it is to you. A useful guide in answering the 'how important' question is to think of whether how important the (a) confidentiality (b) integrity and (c) availability of each information 'asset' is to you on a scale of 1(low) to 5(high).

Once you have this, start thinking about how it could go wrong. So, for example:

- how could the confidentiality of each asset be breached? Could

someone steal the data or mistakenly send it to an untrusted party? This tends to be important for personal or private information;
- how could the data be changed, for example through fraud or error? This can be more important for financial, banking or legal documentation;
- how could the data be made unavailable to you, for example through a systems failure? This can be more important for operational information.

Decide how you want to protect against it – and be clear how this is done.

Now you know what data you have, how important it is to you and how it could go wrong, start to challenge how you protect this. Think about:

- challenging your IT team to be clear on how they are managing each risk on the systems;
- challenging your operational teams on how they manage the risk from a process perspective. For example, this could include training staff, monitoring behavior or secondary checks of critical data;
- challenging your third parties, for example custodians, asset managers or IT service providers, on how they protect your data when it is not under your direct control. They will usually have independent audit reports that can evidence their security, but often won't share this unless you ask.

Validate technical controls – intrusive and often. Trust, but verify

From all of this, you will know what your risks are and what measures you have in place to manage and monitor to these. Now find someone to check that they are working. For technical controls, commission a third party to test them. For procedural controls, audit them, either yourself or through a specific internal audit.
Don't forget your third parties, visit them to talk through their assurance reports and what this means to you.

Make sure everyone understands

Technology is important to managing the cyber security risk. There's no doubt of this. However, many of the vulnerabilities a family office will face will be introduced by the actions of senior management and employees. Whether they implement a system before security testing has been done, or click on an email link from an untrusted source, they need to understand what this could mean and what to do if they think they have made a mistake. Your training and awareness program can go beyond simple annual briefings – think how you can make it interesting and really emphasise the threat. Ultimately, your security will depend on how people behave, so make absolutely certain everyone understands this threat and how you'd like them to respond.

Monitor, monitor, monitor – expect the worst and practice how you'll respond.

The days of building a secure wall at the boundary of your systems and hoping the bad guys stay on the outside are gone. With mobile devices, complex supply chains, cloud computing and advances of technology, your boundary walls are becoming less distinct. A 2015 UK Government survey suggested that 75% of small (and 90% of large) organisations had suffered a security incident. So expect a security breach and watch for it.

Monitoring can range for watching for signs of malicious intent in your employees to reviewing systems logs for evidence someone is stealing your data (and there are technologies and services that can help with this).

If you assume that you will have a breach, understand how you will respond and practice this. Build a scenario for your senior management team of a cyber incident and get them to walk through this. You'll be surprised at how reliant you are on a few key individuals or that you don't keep the data to allow you to investigate.

And the rest…

There are many technical controls you'll pick up along the processes outlined above. Some not to forget are:

- **USB** – control who can use USB keys
- **Firewalls** – use firewalls well
- **Anti-virus** – it's not perfect, but a good anti-virus solution can help
- **Email and web browser** – remember email is not a secure medium. Remember web browsers are often the first line of defence, and that an out of date web browser can lead to a cyber incident.
- **Mobile devices** – challenge how you secure these, and whether corporate data is safe on them
- **Wireless** – be careful of untrusted networks (e.g. hotels or airports).
- **Administrators** – remember there will often be someone in your office that can undermine all your security controls – the IT administrator. Treat them well and oversee what they do.
- **Patching** – make certain your systems are up to date

Conclusion

The risk of cyber-attack is growing exponentially as the opportunities presented by technology and improved systems connectivity grow. This threat to information security is an existential threat to many organisations.

Breaches in the confidentiality, integrity or availability of their data are significant, but the loss of customer or stakeholder trust in their service could be terminal.

Securing digital channels is a complex exercise, and one that draws on a range of governance, risk and assurance capabilities as well as in-depth technical and cyber security skills.

Our cost effective services help you to:

- educate your senior management and employees on security threats and how to respond to these;
- architect your risk, policy, technology and standards environments to help you ensure your business operates according to your risk appetite;
- assure your process and technology, giving you independent and timely information on your state of information security compliance;
- manage your security operation, making sure you blend education, architecture and assurance in a way that is appropriate to your operation.

Educate

Effective cyber and information security requires people to behave in the right way. From senior management balancing risk and reward when launching a new service, to software developers deciding whether to deliver on time (without following security checks) or late (with completing full security checks), most of your employees will, at some point, have the opportunity to introduce insecurity into your organisation with a routine decision. We have designed a suite of education, training and awareness services to help your employees and management make the right decision for your organisation. Educating your employees on security threats and helping them develop the right behaviours to respond to these is therefore critical to building and maintaining an effective security programme.

Architect

Building effective security into a fast moving business is a significant challenge. As with any pervasive risk, the key is to understand the 'parameters' within which your decisions on information security should be made and to ensure that everyone understands and operates these. Our security experts can help you combine these parameters into an information security architecture that is relevant and proportionate to your operation.

Assure

Weaknesses in your security controls will appear through error, misconfiguration or the emergence of an entirely new, previously undocumented vulnerability. We have found that these weaknesses arise however diligent you are in building and operating services. Your security programme should therefore rely heavily on a constant process of checking whether your process and technology controls have been designed and operate effectively. This checking could be independent, as a part of internal audit or as a routine part of business and IT operations. However you choose to test, it is of critical importance that you test to identify and address weaknesses. We have over 30 years' experience of testing and assuring security controls. Our team comprises experts that have tested security at large and small organisations.

Manage

Security can be a complex and fast moving area. Understanding the threats, how they apply to you and how to respond requires experience and expertise that is not available to many organisations. We have therefore designed our security management service help make sure you have the right person running your security programme at the right price. Our management services rely almost exclusively on our expert security resource, and combine many of the themes in our 'Educate', 'Architect' and 'Assure' solutions.

Moore Stephens LLP, 150 Aldersgate Street, London EC1A 4AB
T +44 (0)20 7334 9191
www.moorestephens.co.uk

MOORE STEPHENS

DPS32327