Private Bank

citi

Family Offices and Cybersecurity

May 2017

Contents

Author
Edward Marshall
Citi Private Bank

Cybersecurity trends

"Cybersecurity threats continue to grow in volume, complexity, and are increasingly more targeted against specific companies or people where the greatest financial gains can be achieved."
– Larry Zelvin, Global Head, Cybersecurity, Citi

$400B[1]

Estimated annual business losses globally to cybercrime

61%[2]

of cybercrime victims in 2016 were businesses with less than 1,000 employees

50%[2]

increase in the amount of annual ransomware attacks from 2015 to 2016

These are a few staggering statistics that provide insight into the nature of a risk management problem that is often discussed, but whose nature is seldom well-understood. With this backdrop, data breaches continue to increase annually. There is no shortage of news stories describing cyberattacks. In recent years, attacks ran the gamut from: theft of credit card information, exposing of sensitive medical or financial information, hacking the servers that help run the internet, pilfering political documents, and shutting down power generation in parts of a country at war.

One key trend in the cybersecurity landscape is that the threat is actively evolving – the volume and sophistication of threats is increasing. Whereas perpetrators can make countless attempts but only need to succeed once, those affected by cyberattacks face potentially overwhelming effects from just one cybersecurity failure. The hacker threat has expanded beyond opportunistic individuals using common techniques to include nation-state actors and professional cyber criminals that are properly motivated and armed to wreak havoc on information systems.

[1]Brad Deflin, CEO of Total Digital Security
[2]*Verizon 2017 Data Breach Investigations Report*

A unique threat to Family Offices

Family Offices manage tremendous amounts of wealth, representing 8% of the global UHNW population but nearly 50% of global UHNW wealth.[3] In North America alone, there are an estimated 4,500+ Family Offices. Complex and dedicated efforts to ensure cybersecurity are often given insufficient attention within a Family Office unless a serious breach has occurred in the past with the family.

A recent report by Campden Wealth indicated that 15% of Family Offices surveyed were victims of a cyberattack with losses generally of $50,000 or less, with one incident that cost a family more than $10 million.[4] Don't let the lower dollar value of losses fool you into a sense of security. Hackers use these lower numbers as demands so that people will choose payment to get a quick fix versus trying to fix a problem. Hackers are often impatient and often prefer smaller "sure thing" targets versus drawing unwanted additional attention (e.g. the FBI) through very large demands.

Why Family Offices?

Many Family Offices have the "wealth" commensurate with small and medium enterprises, but typically don't put in place the same levels of security, making them lucrative targets for hackers. Unfortunately, the idea that only corporations and governments are at risk from cyberattacks is prevalent. This lack of preparation makes Family Offices an easier target when compared to other institutions or businesses.

However, looking at wealth alone as a predictor of cyberattack threats is myopic. Family Offices face complex cybersecurity challenges because of these six differentiating factors:

Informal governance structure

While Family Offices as institutions have been around for over a century, structurally these entities usually have operated with a flat managerial style with few strict rules dictating day to day operations. There are exceptions to this trend, for example, when one examines Institutional-level Family Offices (net worth $10B+). However, even some of the wealthiest and best-staffed Family Offices lack formalized daily governance. This is in juxtaposition to often well-established corporate governance guidelines seen in the companies that generated the wealth for the principal. As a result, comprehensive rules and regular training on information security best practices are often haphazardly applied, leading to potential vulnerabilities.

Efficient service vs. effective security

In addition to investment management responsibilities, many Family Offices are charged with handling the administrative concerns of the family. Some of those ancillary functions include setting up family meetings, paying bills, arranging travel, and select concierge duties. Principals expect that the professionals in a Family Office are available to work odd hours and respond to task requests as soon as possible. Often, this culture creates a potential for careless mistakes in information security practices and the avoidance of cybersecurity measures if they are deemed to impede response time to the request from the family.

[3]*The Wealth-X World Ultra Wealth Report* 2015-2016. Rep. Wealth-X, 27 Sept. 2016. Web. 27 Mar. 2017.
[4]UBS, and Campden Wealth. *The Global Family Office Report* 2016. Print.

Underinvestment in critical information technology systems

While the corporations that often create the wealth for a family are well-equipped with information technology staff and updated technology, the Family Office is often deprived of the same treatment because they typically operate as separate corporate entities in locations convenient for the Principal and/or access to capital markets.

Heavy reliance on small staff with outsized access to critical data

Rarely do Single Family Offices employ more than ten staff members on a full-time basis because of operating cost concerns. This creates a problem in that this small group of staff members has access to amounts of data that would normally be compartmentalized in a larger organization. Therefore, if there is a breach at the Family Office level, the repercussions can be very serious.

Security risk from external vendors and partners

The significant risks posed by the supply chains of a business are well-documented and have recently come to the attention of financial regulators as a potentially dangerous security vulnerability. Supply chain risks show organizations are only as secure as the weakest link in their vendors, suppliers, and other miscellaneous third parties with which they interact. For example, a major US retailer fell victim to a hacking event, in which 50+ million customer credit card accounts were compromised through a third-party vendor. With a lean staff without proper IT resources and the sometimes cavalier approach to information security by Family Offices, supply chain risks become more amplified for Family Offices.

Fame and publicity

Prominence often accompanies significant wealth and wealth creation. This attention, whether desired or avoided, could make the Family Office a target. Many Single Family Offices are notoriously private and do what they can to stay off the radar, attempting to anonymize and protect the underlying family they serve by choosing generic names and separate LLC entities. Despite these efforts, wealthy individuals can be easily identified making them potentially lucrative targets for cyber criminals.

In this paper we will look at the cybersecurity threats and trends that Family Offices face and examine how Family Offices can look to manage and mitigate those cyber threats as part of a robust risk mitigation program.

Information security threat trends and actors

"The Internet was built for connectivity and speed – not security and protection. For criminals, rogue states and mischievous actors, the digital world has become the "promised land" – low risk and high reward – offering a borderless reach, assured anonymity and defenseless victims who are not allowed to fight back."
– David Lawrence, Founder, RANE

As the world becomes increasingly interconnected and historically "dumb" devices become "smarter" with the addition of network connectivity and computing power, the cyber threat landscape becomes more complex and prevalent. Today, there are many "smart" devices: phones, medical devices, watches, automobiles, thermostats, lightbulbs, and even frying pans. As society innovates, so do the bad actors. Anything connected to a network is a target for hackers and exploitation.

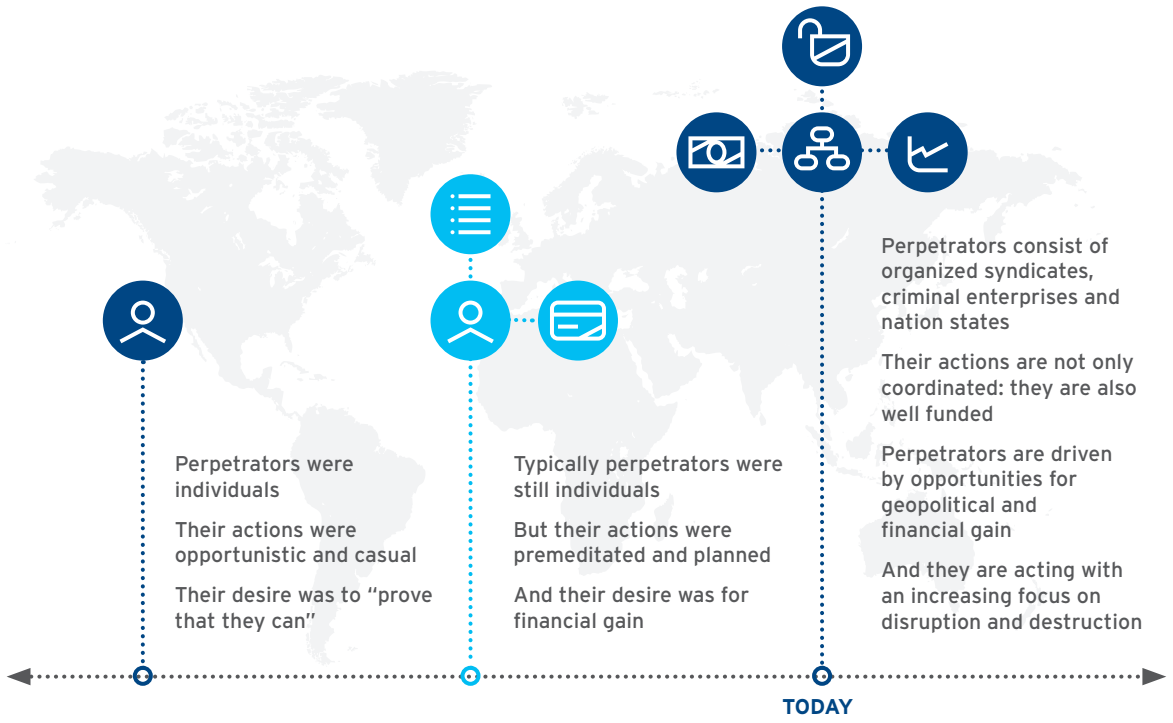


Figure 1: The Changing Information Security Threat Landscape

While there are many areas to explore in terms of information security developments, we believe the following cyberattack trends should be considered critically important to Family Offices because of the threats they pose.

- Ransomware
- Business Email Compromise
- Threats on Social Networking Sites

"There is nothing permanent except change." – Heraclitus

Ransomware

Ransomware denies victims access to critical data and systems. It is often spread through phishing emails containing malicious attachments or "drive-by" downloading – when a victim visits an infected website and malware is downloaded and installed without their knowledge.[5] After ransomware has been executed on a victim's computer, the attacker responsible for the malware demands a ransom payment before allowing the victim to regain access to their systems and data.

A wide scope of industries have started to face ransomware attacks ranging from a hotel that couldn't create new key cards for its rooms, free rides on public transportation because payment systems were overrun, or a police station losing evidence that was stored digitally. Moreover, individuals have also experienced ransomware attacks in the form of attackers threatening to share compromising pictures taken from an exploited laptop camera or threats to post personal data online.

Ransomware attacks have become increasingly pervasive and dollar losses have reached unprecedented levels. There have been over 4,000 new ransomware attacks on any given day since January 1, 2016 – a 300-percent increase over 2015.[6] The FBI believes $209 million was lost in ransomware attacks during just the first three months of 2016,[7] already eclipsing the $1.6 million total losses for all of 2015.[8] These figures are ransoms alone, and don't include costs associated with lost business or network remediation.

The threat is forecast to continue growing given it is easy for attackers to use and has a high rate of return on investment. Simply put, criminals will continue to launch ransomware attacks as long as victims continue to pay ransoms, and those ransoms will likely continue to climb in the coming years due to a number of factors – including increased victimization of businesses like Family Offices.

Early ransomware attacks mostly targeted individual consumers and seemed largely opportunistic. By 2016, however, attackers began to focus their efforts on both businesses and individuals, according to observations by the FBI.[9]

Herein lies the problem for Family Offices – they are financial institutions, private individuals with substantial wealth, and quite often the family members they serve are business owners/executives.

A number of factors may converge to bolster this trend. Family Offices and businesses may: have more money to spend on unlocking their data than an individual victim, be more willing to pay because the data is more valuable, be subject to legal obligations or privacy concerns to protect their data, or need to pay to perform critical operational functions. Moreover, because most ransoms are now paid using cryptocurrency, the transactions become very difficult or impossible for law enforcement to investigate after a ransom has been paid.

Businesses reliant on access to information systems – for things like client lists, shipping databases, etc. – can be crippled by losing their data. As with attacks on consumers, the majority of ransomware campaigns targeting businesses are carried out indiscriminately, but a growing number of victims appear to be carefully selected and targeted because the business is known to run a vulnerable version of a specific piece of software, or simply because the attacker thinks they can extort the business for a high payout.

Modern cyber criminals are even adapting ransomware into business models that mirror legitimate businesses. Ransomware-as-a-Service (RaaS) – loosely based on the Software-as-a-Service (SaaS) model currently popular across the tech industry – is a concept in which ransomware developers offer their software to other cyber criminals as a service under various licensing or profit sharing models, providing their criminal customers with the kind of easy, inexpensive and worry-free computing power on demand that has made SaaS so popular in legitimate industries.

[5] US-CERT; Alert TA14-295A; 22 OCT 14
[6] FBI, *"How to Protect Your Networks from Ransomware"*
[7] FBI source quoted in media reports
[8] FBI, *"2015 Internet Crime Report"*
[9] FBI, *"Incidents of Ransomware on the Rise,"* 29 April 2016

Flexibility in the payment methods for these "affiliate programs" can be beneficial to both parties. Cyber criminals who currently have access to potential victims – such as spammers, botnet operators and watering hole attackers – can now add ransomware to the suite of malware delivered to victim machines at a cost likely lower than developing the malware themselves. Ransomware developers also benefit by gaining access to mechanisms that deliver their malware to large numbers of victims and thereby monetize their malicious code.

Citi analysts expect the ransomware industry to continue growing and evolving, fueled by ease of use, high profits and new business models. How can you protect yourself and your company from this threat?

Best practices for ransomware protection

Begin by preventing ransomware from ever reaching your systems. Employee awareness and training efforts are a critical first step to preventing ransomware, as employees who can identify and properly handle phishing emails delivering ransomware can prevent many ransomware infections.

- **Check the address:** Did that email come from "@myvendor.com" or "@myvend0r.com?" Check email addresses for accuracy and look for anything suspicious, like improper formatting or misspelled names.
- **Avoid clicking on links:** Avoid clicking links in email altogether. If you must click the link, place your cursor over the link before clicking and observe the destination URL at the bottom left of your screen. When in doubt, Google the website you need instead of clicking the link.
- **Be wary of attachments:** Never open attachments from senders you do not recognize. When you do know the recipient, it is still wise to treat any attachment you didn't request as suspicious.
- **Do not conduct any personal business with your work email address:** Avoid situations in which you might be tempted to click on emails related to issues like package delivery or other personal matters.

In the event ransomware interacts with your systems, make sure security "best practices" are followed to minimize the chances it will be installed. Keeping your systems current on updates and security patches, disabling macros in Microsoft Office, and running antivirus software can help catch ransomware that isn't caught by your employees.

Finally, it is important to regularly backup critical data to mitigate a potential successful ransomware attack. Having a data backup and recovery plan for all critical information renders the extortionist's demands ineffectual. This could entail keeping copies of important files safe on an offline storage disk, or having a clean version of your operating system handy in case the machine itself becomes locked entirely.

Reaching out for professional and law enforcement assistance is critical in the event of a ransomware infection. Simply paying the ransom and resuming business may leave some issues unresolved, such as possible continued attacker access to your systems and any associated theft of sensitive data.

It is important to note there are pitfalls associated with paying the ransom that make prevention all the more critical, such as no guarantees the attackers will release your data after you pay, and paying may increase the likelihood of being targeted for ransomware again.

Following these tips can increase your readiness, but ultimately the only way to effectively combat ransomware is to collectively stop paying, as doing so only serves to validate the cyber criminal's business model.

150-250 days[10]

average time it takes for a network breach to be detected (and an average of 50+ days to mitigate the breach)

[10] Jeff Castelli, Accenture Federal Services

Business email compromise[11]

Businesses globally continue to be impacted by a long-standing scheme that exploits executive email accounts and email-based invoicing procedures to execute fraudulent wire transfer payments to foreign banks. This attack traditionally targets how your business processes wire transfers and exploits vulnerabilities in those procedures. As awareness is increasing among victims, actors have recently focused on also compromising sensitive data along with redirection of wires.

U.S. law enforcement reports that Business Email Compromise (BEC) actors are evolving their tactics and becoming more sophisticated. Since late 2013, global law enforcement agencies have been tracking a scheme known as the BEC scam impacting a wide range of businesses and individuals. There has been an explosive increase in identified exposed losses since January 2015. The scam includes multiple types of fraud schemes that all focus on facilitation of fraudulent wire transfers. It remains largely unknown how victims are selected by BEC actors, but several victims have recently reported infections of ransomware immediately preceding a BEC incident. Recently, law enforcement recommended that organizations globally be aware of sudden changes in business practices, specifically colleagues requesting to be contacted on personal email accounts. Communication channel management and verification is an ongoing defensive tool against BEC schemes.

Victims have recently reported a new scenario which involves fraudulent requests from a compromised business executive's email account to internal HR, finance or auditing staff to compromise W-2 data or employee Personally Identifiable Information (PII). These requests for PII may or may not occur along with a request for a fraudulent wire transfer. Law enforcement reports that victims have fallen for this data loss scenario, even if they were able to previously identify traditional incidents of attempted fraudulent wire transfers.

Law enforcement and security researchers concur in openly available reports that the primary BEC scenario involves the compromise of a senior executive's corporate email account or the impersonation of a senior executive's corporate email address. An email appearing to be from the executive is sent to an individual who is responsible for processing wire transfers with a message to process the transaction immediately. This scenario relies upon executive-level authority to authorize such a transaction and conveys a sense of urgency so the employee will execute the fraudulent wire transfer without double checking the authenticity of the request.

There are other versions of the BEC scenario, one of which involves impersonation of a supplier with a longstanding relationship with a business. The business is asked via email, phone or fax for payments to be wire transferred to a new account. If the business receives an email request for the transfer, it will likely be from a fraudulent email address, but closely resemble a familiar email address of the supplier. An example is the transposing of characters in an email address to obscure the sender that at first glance may be difficult to detect — johnasmith@gmail.com vs. johncsmith@gmail.com.

BEC fraudsters can also compromise an employee's personal email account and steal information detailing how the business engages with suppliers, including who the business' point of contact is at the supplier. Using this information, the BEC actor will issue invoices from the compromised business employee's personal email account to the supplier and include new instructions for where to send fraudulent wire transfer payments.

Another variation of the BEC scheme involves victims receiving emails or phone calls from fraudsters impersonating lawyers or representatives of law firms claiming to be working on confidential matters that require the victim to immediately process wire transfers. Victims have reported that this variation of the scheme typically occurs at the end of the business day or week.

As public knowledge about the BEC scheme has expanded, actors are using the following sophisticated tactics to make their activity more difficult to detect:

- Actors have an intimate knowledge of how the victim organization processes internal wire transfer orders.
- When the actors compromise a victim's email account, they use rules to forward emails about their activity to hidden folders or files, making detection by the victim complex and unlikely.
- BEC actors have been observed waiting until executives are on vacation to act, relying on the fact that because these individuals are out of the office, employees will be less likely to question why the executive is emailing them instructions outside of the normal operating procedures and more likely to facilitate a fraudulent wire transfer.

As of June 2016, total global losses from the BEC scheme were over $3 billion, with over 22,000 victims, according to data collected by U.S. law enforcement. Experts agree that the total victim and loss figures are low due to underreporting and that the total losses will continue to increase. Citi clients, along with customers of all financial institutions, are at risk of falling victim to this scheme. Organizations that deploy robust defensive techniques, and particularly those that focus on awareness of the threat with employees that actually receive and process transaction requests, have proven successful in identifying BEC attempts.

[11] *The Business Email Compromise Scheme.* Citi. October 2016

Best practices to counter BEC schemes

- Avoid using publicly available email accounts for business purposes. Entities with open-source email accounts are the most targeted in BEC schemes as these accounts are easiest for the attackers to access and impersonate.
- Closely examine email addresses. Ensure that you check the entire email address and do not rely upon shortened addresses that some email providers substitute for the actual address — e.g. JohnSmith instead of john.smith@gmail.com.
- The field following the @ sign in an email address is known as the domain name. When using a corporate email account, consider filtering email traffic to flag emails from domain names that are similar, but not identical, to either your domain name or your customer domain names. When possible, consider purchasing domain names that are similar, but not identical, to your company name to ensure these variations are not exploited for nefarious use — e.g. a legitimate domain: company-a.com and a possible attacker domain: company_a.com.
- For individuals in the company who have been previously targeted, consider eliminating their ability to use the "Reply" function in email transaction requests. Instead, rely upon a secure list of addresses for contacts that are physically typed in during every email exchange.
- Determine if the number of individuals in your organization who have the authority to approve or conduct wire transfers can be reduced.
- Consider implementing procedures for verifying urgent or confidential wire transfer orders to eliminate this often used technique.
- Explore a second factor authentication method for receiving internal wire transfer requests. This can be as simple as a phone call or as sophisticated as a PIN system to authenticate the user placing the wire transfer request. This will enable the payment processor to authenticate if the transfer order comes from an authorized requester or if the legitimate email account is being used by an unauthorized user.
- Closely monitor high value transactions, new trading partners, new bank or account numbers, and transfers to any new countries. Once thresholds are established, implement maker/checker requirements to ensure anomalies are not overlooked in processing wire transfer orders.

Threats on social networking sites

Social networking sites (SNS), such as LinkedIn, Facebook, Instagram, Twitter, have exploded in the past decade, becoming one of the preeminent modes of communications for both individuals and businesses. Because they are largely unmanaged by businesses, incredibly easy to use and globally scalable, they present both an unprecedented opportunity to businesses from a marketing, branding and customer engagement perspective as well as an unprecedented threat from a cybersecurity, brand risk and compliance perspective. Family Offices face issues from SNSs both from staff at the Family Office and from family members themselves. Based on current customers and market trends, Rubica (a digital security firm for High Net Worth Individuals) believes that individuals with over $5mm in net worth will have a nearly 90% chance of experiencing cybercrime loss with an average amount of $75,000 by 2020. Recent cyber espionage activity and reputation-level impact at other institutions calls for Family Offices to seek to take additional steps to secure these platforms.

Traditionally, the threat from SNSs for Family Offices focused on exposure of a family's whereabouts which could lead to problems of theft, kidnapping or violence against family members. SNSs threats to Family Offices have evolved to provide another door for cyber criminals to infect networks, extract sensitive information or impersonate prominent individuals. Family Offices should address incoming cyber threats leveraging SNSs — ensure the security of official accounts, mitigate staff posting negligent or non-compliant content, find and eliminate scammers exploiting customers, navigate reputational risks, thwart physical threats, and protect against malicious or sensitive information posted to Family Office owned SNS.[12]

Often, Family Offices will downplay the risks stemming from SNSs by discussing their infrequent low usage of SNSs. This opinion is a form of cognitive bias and ignores several factors of cyberattacks that originate on SNSs. Firstly, cyber criminals that target businesses and Family Offices tend to work in complex organized crime networks. These criminal

[12]Evan Blair, Co-Founder of ZeroFOX (www.zerofox.com)

networks write programs that estimate your net worth based on largely publically available information and use highly sophisticated attack methods to infect SNSs. Moreover, there is a market for the programs that allow cyber criminals to conduct these SNS attacks. Secondly, SNSs are becoming more effective at profiling users. This profiling provides substantial demographic and net worth information that can be used to target heads of families through children, relatives and staff.[13] Roderick Jones, CEO of Rubica, recommends a multi-layered approach to protecting families from cyberattacks on SNSs stating: "Human criminals use software to conduct cybercrime on SNSs. These criminals can easily outsmart a software-only defense. The best protection is one that puts humans on the front lines, continually monitoring data streams, looking for anomalies or unsafe behavior, and blocking them in real-time." Lastly, Roderick recommends that families use a virtual private network (VPN) application to increase security while using SNSs, a service that Rubica provides to its clients.

Evan Blair, Co-Founder of ZeroFOX (a social media and digital security firm) believes that Family Offices, at a very minimum, should harden their owned SNS and login credentials to ensure that they are never hijacked by malicious actors. "This is a surprisingly common occurrence, especially for smaller, less followed accounts, and safeguarding SNSs is a simple first step in addressing the overarching risk." Evan recommends that admins within networks monitor privacy settings, enable two-factor authentications and regularly update passwords. Critical staff must be trained on what emails or direct messages to avoid clicking on, especially in the case of an attacker imitating the SNS to steal account credentials.

Once a Family Office has robust controls in place around the official accounts and social assets, they must address the myriad of other inbound and outbound risks on SNS. Inbound risks include social engineering attacks and scams. Evan reminds us that "attackers will also build fake SNS profiles impersonating celebrities, executives or brands and engage with vendors and customers, asking them to reset passwords or disclose financial data". More nefarious actors leverage SNSs to send malware exploits and phishing links via the sites to employees, ultimately infecting networks and extracting valuable information. These attacks exploit the weakest link in any security posture: people. Moreover, they thrive where Family Office employees and families often spend much of their time; online, engaging with friends, family, co-workers and other companies.

Best practices to counter threats from social networking sites (SNSs)[14]

- Use a cyber security service that uses a VPN to monitor, protect and keep private the data of all people that have access to sensitive information.
- Conduct cyber audits to be sure all your people, devices and sensitive information are secure.
- Regularly change passwords and ensure that passwords are not duplicated on multiple SNSs or other sensitive platforms such as corporate accounts, bank accounts and personal email accounts.
- Enable multi-factor authentication, when available. This feature is oftentimes offered by popular SNSs; however the user must elect to activate the feature. This can be found in the SNS help tab or search bar.
- Be vigilant of connection requests from users, even those with established connections to family or friends within your network. Fraudsters posing as legitimate contacts are very active on social media.
- Train employees to identify social engineering attacks, malicious posts, and how and what to post publicly. Create a process for both staff and customers to report malicious activity that can then be passed to the SNSs.
- Regularly check for external accounts imitating the company or people within the company, and monitor for malicious links posted to pages or in direct messages.
- Maintain familiarity with the privacy filters and rules to ensure awareness of how your content is being shared. Changes are frequently made by the SNSs, requiring periodic attention by the user to the settings. Set your privacy filters at the highest levels.
- Do not click on any links within email messages or direct messages claiming to be from the SNS themselves. Links like these redirect to pages that imitate the SNS login page to harvest credentials.
- Consider an automated tool to monitor for external threats, such as malicious links, scams, violent language and fraudulent accounts using your name, logo and messaging. These violate SNS terms of service and can be taken down if identified. This data can inform other areas of the business like physical security or marketing and provides a hands off way to ensure safety on SNSs.

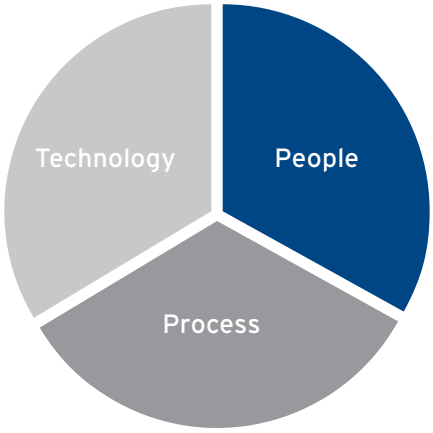
[13]Roderick Jones, CEO of Rubica (www.rubica.com)
[14]Evan Blair, Co-Founder of ZeroFOX (www.zerofox.com)

What Family Offices can do today

"Prophesy is a good line of business, but it is full of risks."
– Mark Twain

News headlines and the steady drumbeat of warnings of the consequences of improperly preparing against cybersecurity risks have made the threats look like a hydra – tackle one problem and two more appear. Family Offices are asking: What should we focus on? Is protection against the threats worth the expenditure? Who can we trust in the cybersecurity market? Are there benchmarks from other sectors we can emulate?

Regardless of what stage of cybersecurity preparedness Family Offices find themselves in, they should start developing a comprehensive information security program that is flexible and can incorporate lessons learned and adapt to new threats. We recommend that Family Offices consider a framework based on 1) technology, 2) people, and 3) process when implementing and improving their cybersecurity programs.



Too often families will sacrifice training over a new hot technology service or ignore simple improvements like annually checking their staff's software and devices to make sure they are updated. Furthermore, Family Offices need to identify what and where critical digital assets are. Family Offices have to understand what the "crown jewels" are and determine if they are safe, even if their network has been breached.

Bob Butler, Senior Vice President for Critical Infrastructure Protection Operations at AECOM, has a background that spans 35+ years of experience looking at this problem with unique experiences in the national security community and industry. "As the Chief Security Officer of a global data center company with nearly 700 clients, I found building cyber security capabilities to prevent and counter breaches to be very expensive. A key question for our Board and me was where could we get the most 'security' for the dollar invested. Critical to answering that question was the use of a comprehensive and company-tailored risk analysis process that continuously assessed threats to clients, corporate tech vulnerabilities and the consequences of breach."[15]

Family Offices face resource constraints similar to corporations and we provide a few possible areas for consideration to build resilient and secure organizations.

[15]Bob Butler, Chief Security Advisor for Cyber Strategies LLC.

Family Office information security training and policies

People are often the weakest link in the information security system for a Family Office. The level of awareness on information security threats and the proper ways to combat them has great variability. Therefore, cybersecurity education should be a key part of family planning and business operations meetings.

"The best defensive technology in the world doesn't protect you from your weakest link — the people that use it. Security policies and training from the board room to the break room are imperative to any risk mitigation plan. Decades of exponential progress in digital technology have created an environment where individual experience and intuition fail to serve and keep pace. Change will continue to accelerate and life-long learning that is aligned with adaptation and agility skills is required for survival and success. For now, nowhere is this more evident than in cyber safety and information security. Cyber risk is now an existential threat. Personally, professionally, it never goes away. Effective training is about individuals, cyber self-defense, and their long-term quality of life."[16]

Another simple way to help shore up cyber defenses is through the creation of Family Office cybersecurity policies. These policies can be derivations from parent companies that created the wealth that are customized to the unique nature of the Family Office. Policies should include recommendations on how to prevent cyberattacks and what to do in case a breach is detected. Policies should be updated regularly and Family Office teams should regularly certify that all members (including the Principal) understand the policies and procedures. Figure 2 provides a broad framework for families to consider as they build an Information Security policy document.

Family Offices should also consider working with internal or external partners to test staff awareness of these policies.

Figure 2: Family Office information security — policy checklist

- ☐ Regularly back up your data off-site
- ☐ Change passwords regularly
- ☐ Use a password manager to avoid using the same password for applications
- ☐ Use two-factor authentication when possible to verify instructions
- ☐ Automate software updates on all electronic devices
- ☐ Never send unencrypted emails that contain personal information such as credit card numbers, addresses, birth dates and social security numbers
- ☐ Use Virtual Private Network (VPN) services when using Family Office or personal devices

For example, a family could work with internal teams or hire an outside vendor to perform "white hat" simulated cyberattack tests against staff to determine weak points and increase general understanding of threats.

These tests are usually "pretend" malicious attachments, Tweets and Facebook messages with pretend malicious shortened URLs. If a Family Office staff member clicks on the link, they typically will get a "gotcha" surprise. Regardless of the type of training, Family Offices should consider refreshing and educating no less than on a quarterly basis.

$75,000[17]

average cybercrime loss experienced by families with a net worth of more than $10mm

[16]Brad Deflin, CEO of Total Digital Security
[17]Roderick Jones, CEO of Rubica

Secure your communications

Cybersecurity threats regularly impact individuals on their corporate and personal devices and a heightened level of security and awareness is necessary on both kinds of devices. As employees increasingly participate in corporate Bring Your Own Device programs, the line is blurred between personal and corporate communications as corporate data is regularly accessed through or across personal devices. The following list of industry best practices is not an exhaustive list but may help reduce your risk of a security breach.

On personal devices:

- Ensure you access corporate data using only those security tools implemented by your organization. Do not circumvent these tools by using webmail or connecting to the corporate network outside of a secure connection. Do not store sensitive corporate information on personal devices. Whenever possible, promote separation between resources used for work and personal matters.
- Avoid using free public Wi-Fi connections. If this is unavoidable consider using a commercially available VPN solution on your personally owned computer and mobile devices to prevent the capture of your data stream.
- Exercise extreme vigilance when clicking on any links or opening attachments. If any of the following elements are out of the ordinary, do not click on the link or open the attachment — time sent, minor variations in the email address, file name, or actual web address of the link embedded in the email. In the event that you do click on a suspicious link or attachment do not use the device until you run a virus scan and perform any necessary clean up recommendations.
- Update the mobile device or laptop operating system when told to do so by system update messages.
- Ensure that you are using an Internet browser that is updated.

Cyber insurance

While cyber insurance is a burgeoning field for insurance companies and corporations, it can serve as another potential line of defense for Family Offices. Insurance, at its core, is a risk management tool, and with an evolving threat stemming from information security, Cyber Insurance presents an opportunity for Family Offices to evaluate gaps and build customized solutions.

Cyber Insurance requires an underwriting process and this is an aspect that Family Offices should explore as well. While actuarial data for cyber insurance is in its infancy compared to more established lines, underwriting practices are being improved as the size of the market grows, threats expand, and the attack data sets are analyzed.

Going through an underwriting process with an insurance broker and carrier can provide Family Offices with a better understanding of the current state of cybersecurity issues and standings against industry benchmarks.

Ben Beeson, who runs the Cyber Risk Practice for Lockton Companies, a global insurance broker, believes that balance is important when building effective resilience throughout Family Offices. "Investment in controls that seek to mitigate threats remains important but every Family Office should expect that they still may be compromised regardless of the level of this investment. In this context a strategy is needed that seeks to minimize the size of financial loss to you if an incident occurs and, as a consequence, this strategy should also now include insurance acquisition."[18]

Cyber Insurance coverage can be tailored based on the needs of the Family Office. Be sure you understand the fine print of any insurance policy you choose to explore. Some of them have exclusions on certain types of attacks such as ransomware. Beeson believes a Family Office should explore these key components of cyber coverage:

- **Breach response** costs that may involve the need to notify employees whose personal data has been stolen or your engagement of an IT forensic expert to identify and remediate the problem.
- **Cyber extortion** costs involved in responding to a ransomware attack that has encrypted your data.
- **Network interruption** costs following a distributed denial of service attack that has brought down your computer network.
- **Data restoration** costs involved in restoring stolen or compromised data.

[18]Ben Beeson, Cyber Risk Practice Leader, Lockton, Inc.

Active cybersecurity due diligence on external suppliers, vendors and staff[19]

As discussed earlier, supply chain risks are particularly important for Family Offices to consider. Third-party risks — the notion that a contractor or a supplier could inadvertently expose the first-party organization to a network breach — are a tangible and growing concern. However, while many larger companies are cognizant of third-party risk, actually addressing this emerging concern is not yet a high priority in the Family Office space. It should be, especially among Family Offices who bring on third-party vendors and consultants.

Family offices face these risks because they are often not equipped to enforce and validate the security policies on those third parties. Larger companies are in a position to enforce stringent, expert-developed security policies on vendors, and have a strong assessment program and processes to be sure their third parties have strong security policy and practices. Family Offices, on the other hand, are generally at the mercy of generalists, who may not be as proficient at advanced security practice. Also, Family Offices are generally priced out of the high-end security market, and forced to rely on smaller pools of locally available vendors and consultants.

Family Office staff should consider working with internal and external partners to conduct cybersecurity due diligence before and during an engagement. Checking early and often will help Family Offices avoid neglecting unexpected holes in their cybersecurity defenses. Below are some recommendations on how Family Offices can reduce risk exposure against threats from third parties:

1. During the on-boarding of the third party, the contractual agreement should outline how the third party secures sensitive data
2. Family Offices should consider hiring larger and more well-known third parties as they are well established and may have better security practices
3. Family Offices should consider working with third-party services that use strict security measures to protect their data and those that are able to demonstrate effectiveness through internal and external assessments
4. Family Offices should ask vendors if they carry a cyber insurance policy and have specific provisions related to their financial and reputation risk
5. Family Offices should also deploy strong security policy and practices to reduce the risk from the third-party contractor and employees, including a strong password policy, limited privileged access to network and applications, and a vendor security log review program

Coordinate with other Family Offices

By their nature, Family Offices are discrete, often maintaining reduced public profiles. However, these organizations are often willing to meet and network with other Family Offices to share intelligence. This data sharing is typically of the investment nature or concerning next generation issues. Family Offices would benefit from expanding intelligence sharing to include cybersecurity issues.

"After identifying strategies to protect the most important information assets, I found I could significantly increase my awareness of and counter cyber threats by setting up a trusted information sharing exchange, leveraging the cybersecurity investments of our client base and with other data centers. As increasingly sophisticated cyber criminals take greater aim at high net worth Family Offices, building a collective and proactive self-defense, based on sharing cyber threat information and best practices across Family Offices, should be foundational for any Family Office business operation."[20]

As Family Offices become distinct and visible, numerous conferences have emerged to cater to this group both in the US and abroad. Family Offices should also consider adding information security conferences to their annual circuit such as the RSA Conference, Black Hat, SANS, Spooks and Suits, or Infosecurity Europe.

As awareness grows, so does proliferation of published information on cybersecurity issues for Family Offices. Staff should regularly view cybersecurity information from Family Office associations, webinars, podcasts, and on LinkedIn. Family Offices should also examine information from private and public organizations such as: APWG (http://www.antiphishing.org), ISACA (https://www.isaca.org), No More Ransom Project (https://www.nomoreransom.org), the Cyber Threat Alliance (https://cyberthreatalliance.org), the Pew Research Center (http://www.pewinternet.org/quiz/cybersecurity-knowledge/), the Department of Homeland Security (https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks) or the FBI (https://www.fbi.gov/investigate/cyber).

There is also a cottage industry of security professionals and organizations springing up that cater to Family Office security and specifically cybersecurity issues. "Family Offices now join the largest public companies in trying to protect their cash, IP,

[19]Kambiz Mofrad, GIS Third Party Information Security Assessments, Citigroup
[20]Bob Butler, Chief Security Advisor for Cyber Strategies LLC.

brand, reputation, sensitive information, M&A data, etc. from hackers. With cyber and IoT providing bad actors more access points than ever to wreak havoc, we are seeing an all-out war for security talent. Some of the most in demand experts come from the highest levels of the Intelligence Community and Special Operations community. They know the playbook of the information security adversaries," said Jeremy King, president of Benchmark Executive Search, a firm that specializes in placing cybersecurity executives and staff.

Family Offices should contact their attorneys, accountants, corporate Chief Information Security Officers (CISOs), and other professionals to identify suitable cybersecurity partners.

Nate Fick, CEO of Endgame, a cybersecurity technology company that aims to turn security operations teams from incident responders to proactive preventers, believes the speed of response to cyberattacks is a critical area to improve. Fick and his team believe that speed will help stop damage and deter cyber attackers instead of the traditional approach to cybersecurity — fighting the adversary on his level and spending a fortune to build an easily bypassed Maginot Line.

Family Offices face a challenging world as cyber criminals look to exploit their very nature. Threats continue to evolve in cyberspace because new defense mechanisms lead to innovative new attacks methods and vectors. Building a resilient, cognizant and learning culture around information security is important for Family Offices of all sizes and jurisdictions.

About the author

Edward V. Marshall is a Director in the Global Family Office Group at Citi Private Bank. Edward advises families of significant wealth on best practices in Family Office and investment management across North America. The Global Family Office Group serves more than 1,200 families around the world, providing a wide range of financial, advisory, and educational resources to Family Offices of all sizes and complexity.

Previously, Edward served as Relationship Manager and member of the ultra high net worth team at Credit Suisse. He started his career in the public sector working for the Federal government in the US and abroad.

Edward has an MBA from New York University's Stern Graduate School of Business and a B.S. in Human Biology from Michigan State University. He speaks Polish, Russian and Ukrainian.