FAMILY WEALTH REPORT
from WealthBriefing

Guest Feature: Cybersecurity Basics For The Family Office - Part One

ANNMARIE GIBLIN
September 13, 2016

This is the first half of a two-part feature by Annmarie Giblin and Theresa Pratt looking at cybersecurity best practices for family offices. Based in New York, Giblin - who has written part one - works at a US law firm while Pratt is director of IT at Market Street Trust Company.

These views belong solely to the authors and are meant for information purposes only; this article is not meant to provide or be used as legal advice.

Cybersecurity is an area of increasing focus and concern for the family office. It can also be a confusing and difficult area for the family office, where allocation of assets is always a concern and defining where to invest the same in cybersecurity is not always crystal clear. Indeed, a family office is charged with more than protecting wealth, but also ensuring legacy, reputation and relationships. In the past, the family office could insulate itself to some degree with discretion and proper hiring. This is no longer the case. Family offices must take proactive steps to protect themselves now to help to prevent a cybersecurity incident and, second, to minimize the damage should one occur.

To further complicate this area, the aftermath of several high profile cybersecurity incidents and the government's increased focus on this area has created a lot of noise about cybersecurity best practices and incident response. This article will attempt to quiet some of that noise by providing the general legal perspective of what a solid cybersecurity program should include, combined with the boots on the ground realities of implementation.

It is important to realize that cybersecurity, and security in general, is not a one-size-fits-all program. Each family office or multi-family office must tailor its cybersecurity program to fit the personality and needs of the office. It is also important to continually evaluate the office's approach to cybersecurity for needed changes on an annual basis to ensure that the program is keeping up with the growth and needs of the office. However, there are some general and basic steps that can be taken to ensure a basic level of protection in whichever program best fits the individual office's needs.

Back to basics – what is cybersecurity?

According to TechTarget.com, "Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity." It is common for the word cyber to receive too much focus in this area. Instead, the focus should be on "security," which is the fundamental goal of any cybersecurity program.

Technology has made life much easier, but also has created a back door to information. The explosion of mobile technology has further complicated this area, as our smart phones and tablets, items of great enjoyment and convenience, make our information systems that much more vulnerable. If you think of the family office as a home, cybersecurity is the unlocked and unalarmed back door. A criminal just needs to figure out how to open the door and

they are in the home. The goal is to secure that door as much as possible, and, further, protect the most valuable information as you would your valued possessions in the event that they get in.

Preparing for the worst, hoping for the best – the legal perspective

From a legal perspective, it is best to assume that the family office will be the victim of a cybersecurity incident and prepare for the same. It is much better to be over-prepared and ready for the aftermath, then left holding the bag when an incident occurs. Of course, a scorch earth policy is not required and, as noted above, each office needs to tailor an approach best suited to address its security concerns. There are, however, several universal actions that can be taken to put the family office in the best position possible to deal with and protect against a cybersecurity incident. Regardless of the family office's approach to cybersecurity, or security in general, it is imperative that the family office has a plan in place. In today's legal and regulatory landscape, not having a cybersecurity program is no longer acceptable.

As an initial first step in this process (whether starting a security program from scratch or taking a fresh look at the one already in place), is to create an "information inventory." An information inventory identifies what information the office maintains and why. Once the information is identified, then it must be organized into categories of importance, so that the most sensitive information can be identified and heavily protected. Using the house example above, this is akin to putting expensive jewelry in a safe in the event of a burglar breaking in. This is much easier said than done, especially if dealing with a multi-generational family office that is still using legacy systems, but it must be done nonetheless. Indeed, if the family office is the victim of an incident, the only way to know what was taken is to know what you had. Without this fundamental information inventory, there is no way to effectively protect the most sensitive information and ensure that it has not been compromised in the event of an incident.

This is also an important step for the family office to actually know what information it is maintaining and why. This exercise may reveal that resources are being wasted on keeping irrelevant or useless information. It may also reveal information being maintained that is not supposed to be within the office. Most importantly, when completed, the information inventory will help to streamline the cybersecurity processes and help to put in place effective security.

Second, once the inventory is complete, the information identified needs to be protected. Remember that, when putting these security policies into place, it is important to not forget physical security. Sensitive information can still be stolen from a piece of paper. Ensure that any cybersecurity program identifies the physical threat as well as the virtual, and considers both when putting protections into place. In the same way that you would not use a shotgun to kill a housefly, there is no need to protect all of the information maintained by the family office in the same manner. Overkill can not only be useless, but extremely expensive. Thus, a layered system is likely the best way to ensure all the information is protected, with the most sensitive and important information receiving the strongest security. In order to do this, the family office will need a data retention policy ("DRP"), an incident response plan ("IRP") and a team of professionals to implement them both.

The DRP should be an outline of what general types of information the family office keeps, where this information is kept and why. The DRP should include a time frame for the storing of documents and the destruction of the same. The DRP does not have to be overly detailed and should be at the very least a general blueprint for the data collected and maintained by the family office.

The IRP should detail what the office will do in the event of a cybersecurity incident. The IRP needs to be as detailed as possible to ensure that when an incident occurs the plan goes into effect immediately to stop the attack/loss of information, and find out what was taken. The IRP also needs to address the aftermath: insurance policy information so notice can be provided; necessary contacts (i.e. attorney, law enforcement, forensics, key family

members, PR personnel, etc.); which breach notification laws must be complied with and the time frame for the same; preparation for potential litigation and regulatory hearings, etc. The IRP is a fluid document, and should be tested and updated as much as possible. Time is of the essence in a cybersecurity incident and the IRP should allow the response to an incident to start as soon as possible.

Both the IRP and DRP need to account for third parties/vendors that the office shares its information with. Indeed, not only are third parties potential sources of an incident, but these relationships are being examined very closely by regulators now. Include not only a system for the sharing of information with third parties, but also a way to recover or provide for the destruction of the same after the information is no longer needed by the third party.

Ensure that the employees of the office are familiar with the DRP and the IRP. Conduct annual training to ensure that both are being adhered to and that best security practices are being followed. A family office or any business for that matter can have the best policies on paper, but if they are not being followed, or if the employees are not familiar with them, they are useless.

In addition to the DRP and the IRP, each family office should have a cybersecurity team. Ideally, the cybersecurity team will include outside professionals who are familiar with the office's DRP and IRP (hopefully having been a part of drafting or testing of the IRP), who are be ready to implement it in the event of a cybersecurity incident. The team at the very least should include a forensics professional and outside counsel. If possible, the team would also include a PR professional and an insurance professional. The team can also include anyone else essential to getting the office back to business, which can mean different things for each office. Importantly, the team should be assembled and practiced before an incident.

It is important to note that bringing in outside counsel and forensics professionals is very important in the event of a cybersecurity incident. Outside counsel can not only help to guide the legal aspects of the incident response, but also can help to keep certain portions or the entire investigation and response privileged, which will be important in the event of any resulting litigation. Outside forensic professionals are equally important because they will be needed to stop the attack, identify the vulnerability and, if possible, recover the information. Indeed, the family office's own IT team may be too close to the situation to be able to effectively deal with this and/or too overwhelmed with other aspects of the office's systems and will likely need the help.

Finally, test all of the above. An IRP needs to be tested to reveal any holes that only a real world situation can show. The family office should work a cyber breach fire drill into its yearly schedule to ensure that the IRP is as tight as possible and effectively deals with any real world issues that weren't considered. It will also see how effective the plan is when implemented, which will allow for necessary tweaks. The best way to accomplish this is to only include a few key members of the office in the drill, allowing for everyone else to believe that this is a real life event. These drills along with penetration testing should be an integral part of the overall security plan.

Overall, it is better to be prepared and never have to use the plan than to be underprepared and suffer a greater loss from the incident. Remember that the above is a very general outline of what a cybersecurity program should cover; but a program that does cover at least these basics is a great first step to a more secure and protected family office.

Part two will explore the realities of implantation of a cybersecurity program for the family office.

FAMILY WEALTH REPORT
from WealthBriefing

Guest Feature: Cybersecurity Basics For The Family Office - Part Two

THERESA PRATT
September 15, 2016

This is the second half of a two-part feature by Annmarie Giblin and Theresa Pratt looking at cybersecurity best practices for family offices. Based in New York, Giblin - who wrote part one - works at a US law firm while Pratt is director of IT at Market Street Trust Company.

This article is part two of last week's discussion of the basics of cybersecurity. The previous article, which can be viewed here, explored the legal best practices related to cybersecurity and discussed key concepts like having an information inventory, data retention policy, incident response plan and a response team. These are all very important, and nothing said now should be taken to minimize how critical they are.

As the definition of cybersecurity from TechTarget.com suggests, proper cybersecurity is one third technology and two-thirds practices and procedures. Due to my role as IT director, I take security very seriously and that carries over to how I protect my home and possessions. We have a security system, cameras and other "techy" items in place to protect us. None of these are helpful however, when I come home and find the house is unlocked and my spouse has left his login names and passwords, written out on a piece of paper, laying on the coffee table. My flashy cameras are useless without the policy of not writing passwords on paper and the practice of locking the door when we leave. These three must work symbiotically to achieve effective cybersecurity.

There are some realities of "boots on the ground" running a family office that are, in my opinion, unique to this industry. With these in mind, let me augment the comments from part one of this series with a few practical suggestions.

Preparing for the worst, hoping for the best – a realistic perspective

Many family offices are small organizations with limited resources. Obtaining additional resources usually means asking the family, either via the board who is often populated with family members or going directly to the patriarch or matriarch. Additionally, the family members who wield the most control may be in a generation that typically does not understand or fully appreciate cybersecurity. I am of course generalizing and many exceptions apply, but this situation can create a unique challenge for family offices who wish to step up their cybersecurity game. So, as an executive caught in this interesting dilemma, what do you do?

First, training. Train yourself, train your staff, train your board, train your clients. The biggest threat any organization faces, whether large or small, is that someone will click on something bad or take action on a fake or phishing scam. There is not a technology in the world that can protect you from the random clicking of the unwary.

Proper cybersecurity awareness begins with an attitude of "question everything". Are you really sure the email you just received is from your client? And if it is, are you really sure they want you to wire $200,000 for a painting to France? (This is a real example of a fake request we received from a hacked client email account.) Create a mindset of risk management where decisions to act include the question, "Is this action worth the risk?" We receive fake requests

every single day. Fake invoices demanding payment, email requests from “clients” asking for money to be wired, surveys asking for detailed information about our IT infrastructure, phone calls asking for details about staff and/or clients. The list goes on and on. I spend a significant amount of my time as IT director working one on one with staff members, looking at individual situations, determining whether or not they are legitimate and taking advantage of teachable moments. I tell the staff each and every time I would rather answer the same question ten times a day than have them do something that creates a security incident. Your staff is your main line of defense. Tell them that and teach them what to look for.

Training does not have to be expensive. There are many good online resources to help you become and stay aware. The SANS Institute is one of the best resources available. They have a monthly newsletter called OUCH that talks about real cyber threats in plain English. Additionally, they publish a video of the month and have free security awareness posters. The SANS Institute also provides best in class training which can be pricey. This is where the FBI goes for training. CIO.com is another great resource. You can sign up for email alerts that will literally fill your inbox with the latest and greatest of all things technology. As a next step, consider building relationships with your local FBI agents. Generally, the FBI wants to help you become educated and aware. Our local agent has come to the office twice in the past year to provide awareness training to the staff and board. When the FBI says it, the board listens. Once they understand the threats, they are much more likely to approve resources for other, more expensive tools.

Another practical, inexpensive tip is to develop sound cybersecurity practices that everyone understands and follows. Develop a practice of using strong, secure passwords (14+ character phrases) and changing them regularly (at least every 90 days). When using these passphrases, avoid common phrases. We recently hired an outside consultant to test the strength of our passwords, and he was able to crack (in less than 30 seconds) a 14+ character, complex pass-phrase because it was based on a common “greeting card” like statement. Develop a procedure for verifying the requests you receive. If a client emails asking for a wire, verify the request by calling them back on a number you already have. Develop a procedure for sending sensitive information securely (not in the body of an email or as an unencrypted attachment).

Develop a procedure for keeping track of all the visitors in your building, including the regular delivery and service people. Empower your staff to politely confront anyone they do not know or were not expecting. Physical security is very important and many breaches happen because nobody questioned the “FedEx guy” who picked up and walked off with a stack of sensitive papers. The security firm I employ to conduct our penetration testing says they have near 100 per cent success in gaining physical access by posing as UPS and/or FedEx delivery personnel. Implement a clean-desk policy where all sensitive documents must be kept out of sight and under lock and key. Tell your staff, this is our house and it is up to us to protect it.

Once you have taken care of these “low hanging fruit” items, turn your eyes towards the technical.

Make sure every computer in your family office is running anti-virus. This too does not necessarily have to be expensive. Microsoft provides a decent antivirus called Windows Defender for free. It has been part of the operating system since Windows 7. If you already have antivirus, centralize the management of it so you can easily tell if everyone is up to date. Also, know which antivirus you are running and make sure your staff also knows. A very common scheme is called the fake anti-virus. A window will pop up claiming to be your antivirus, but if you click on it – you get a virus. If you know you are running MacAfee, and a Norton window pops up, it is fake and you won’t be fooled. Additionally, consider antivirus on your mobile devices. Norton makes a good one and it is available in the app stores.

Another important thing you can do is implement regular patching. Patch your user computers, patch your servers, update your mobile devices. Keep your internet browsers up to date. Regular patching means weekly patching. Many viruses and infections take advantage of weaknesses that have been known about for a long time. Patches are written

to fix those weaknesses. Applying those patches shores up the deficiencies in your protective armor. There is also what is called the “zero-day exploit” which is when a criminal finds out about a flaw, creates a way to take advantage of it and levels it at you before the fix or patch is available. This type of attack is much less likely so put your resources into protecting yourself from the greater risk by patching regularly. If you do not know how, find a person or a service who does.

A monitoring/management service such as LogMeIn or LabTech can help you stay on top of this so you know for certain the patching has been done. Patching is all too often overlooked, even by much larger organizations. If you are not patching, you are wearing old, broken armor. If you have a legacy system (as in we used to use it, have moved on, but need it for historical purposes) that can no longer be patched or updated, remove it from your network. Place it on a computer that has no internet or network access and require your staff to walk up to it and use it. Therefore, if it is compromised, the virus, hacker or other threat has nowhere to go.

Once you have done these things, turn your eyes to sound, daily back-up procedures, disaster recovery, business continuity, incident response and all of the other very important things discussed previously. Cybersecurity is most effective when implemented in layers. Training, procedures, antivirus and patching provide the foundational layer on which everything else rests.

Conclusion

Cybersecurity is a complicated issue for the family office, and as demonstrated above, not an easy one to address. It is an on-going, evolving subject that requires constant attention and work. Cybersecurity will never be effective if addressed from a “check the box” or a “set it and forget it” mentality. As part one discussed, there is evolving research, thought and best practices that help set the framework for an effective program. This is a new and growing area of legal thought that cannot receive enough attention. This section tried to address the pragmatic realities of managing cybersecurity in an active family office. The best overall approach is to intertwine policies, practices and technology, while being diligent with training and physical security. The unfortunate reality is that a family office will be a victim of a cyber-attack; now is the time to prepare.