TOP 10 INTERNAL CONTROLS TO MITIGATE CYBERSECURITY RISKS IN THE FAMILY OFFICE

CURRENT CYBERSECURITY TRENDS

"It is estimated that by 2027, global spending on cybersecurity will reach $10 billion. In this age of IoT, where there is no escaping the internet, it is very important to understand the importance of cyber security and more importantly, the types of cyber security threats around you!"

– Matt Powell, CPO Magazine

$400B is the estimated annual business loss to cybercrime globally[1]

94% of organizations experienced phishing attacks[2]

73% of organizations impacted by impersonation attacks have experienced a direct loss[3]

These are just a few statistics to provide some perspective on the risk many small businesses and family offices may face. Cybersecurity risks do not just affect corporations and government entities but can be a common and very present danger to family offices and small businesses alike.

1 Brad Deflin, CEO of Total Digital Security
2 Mimecast. The State of Email Security Report 2019
3 Ibid.

WHY ARE FAMILY OFFICES AT RISK?

In addition to the common risks an organization faces, family offices can also be targets for cyberattacks that may not be financially motivated. Compared to the risk most organizations face against cyberattacks, family offices are at increased risk for a cyberattack due to the potential for blackmail, extortion, and smear campaigns.

Employee risk comes from current or former employees who may elect to perpetrate or facilitate an attack, employees who have a sense of entitlement, and long-term, trusted employees who may have extensive access to systems and data. No matter how capable or trustworthy your employees are, human error is the biggest risk in cybersecurity. In fact, 90 percent of breaches are caused by human error rather than software flaws and vulnerabilities.

Family offices are at risk because…

- Family offices manage and represent a tremendous amount of wealth.
- Historically, cybersecurity has not been an area of focused investment for family offices, or these offices lack the levels of security found in larger enterprises.
- Lack of procedures or preparations for internal cybersecurity risks.
- Fewer employees to manage all operations could mean more risk of a cyberattack.

BEST PRACTICES FOR MITIGATING RISK TO THE FAMILY OFFICE

Even the worst cyberattacks have very simple origins: attack vectors. Currently, 92 percent of malware is delivered via email; however, because the types of entry points continue to evolve, many will not be caught by a family office firewall. As a result, employee security awareness training, testing, and auditing is the first line of defense.

As with all organizations, family offices must be diligent in relation to the potential risks posed by current and former employees and relationships with third party vendors, especially those that have some level of access to family office data.

Top 10 Internal Controls Every Family Office Should Have:

1. Having a well-crafted and comprehensive set of policies, procedures, and controls is foundational for any organization, and family offices are no exception. Policies around access management, clear delegation of authority, segregation of duties, and a host of other topics are a must. The policies, procedures, and controls must include family members as part of the overall governance process. Most importantly, just having the policies in place is not sufficient – periodic reviews and reassessments of the policies and controls is a necessary step to ensure adherence.

2. Train your employees, then train them again. Family office employees are the first line of defense when it comes to cyberattacks. Every employee should have a solid awareness of the threats that exist and how to identify them and know what to do if they suspect something. Unfortunately, just having a robust training program in place is not enough. It is critical to test employees to ensure that the training they receive is integrated into day-to-day activities, and it is equally important to audit the results of the training and testing regimen.

3. The use of personal email, social media, document sharing, and document storage devices should be limited, if not prohibited all together. In an effort to avoid an intentional or inadvertent data breach, preventing family office employees from using personal accounts to conduct office business is critical.

4. Email encryption as standard practice. If a family office email system does not encrypt all communications as a matter of course, then a separate system or platform should be used to send communications that contain personal, financial or otherwise sensitive information.

5. Desktops, laptops, and servers must be encrypted at rest. Historically, only devices that could be "mobile" were encrypted as such to prevent data loss in the event of theft of the device. Today, as the cost of technology continues to decrease, the internal hard drives within all devices, including servers, should be encrypted.

6. Secure passwords and log-in information. Confidentiality is paramount. Password and log-in information should be maintained in a secure location such as a password manager app. Be careful what information you share.

7. Maintain a secure and protected vendor list from which access is prohibited for employees in the A/P function. Changes to vendor information should be subject to additional verification and review.

8. Proper vetting and auditing of third party vendor access and activities is a must, and often a task that family offices overlook. Vendor risk comes from allowing an external third party to access systems and the underlying data on those systems.

9. The family office should have a separate insurance policy covering cybersecurity. The family office insurance broker should have full knowledge of the family office structure and policies in place to protect the family office from the financial burden of cyberattacks.

10. Understanding the organization's social media "footprint" and restricting employee use of family office information on their personal social media is critical. Spear phishing campaigns are often based on gleaning critical information from social media. Family offices should instill best practices for maintaining confidentiality.

Be proactive!

- Contact advisors for assessments of internal controls, risk assessment, and insurance review.
- Be aware of who you are letting in.
- Insure the family office and obtain cyber insurance.
- Keep the family and the family business separate in areas such as emails, social media, etc.
- Establish a cybersecurity policy and process, implement safety technology, and train your people.

For more information on Family Office Cybersecurity, reach out to the following advisors:

FAMILY OFFICE SERVICES

JASON CAIN
Family Office Services Managing Partner
312-730-1435 / jcain@bdo.com

AMY PIENTA
Family Office Services Managing Director
312-730-1414 / apienta@bdo.com

CRAIG WITCHER
Family Office Services Managing Director
616-389-8679 / cwitcher@bdo.com

ADVISORY & ASSURANCE SERVICES

GREGORY GARRETT
Head of U.S. and International Cybersecurity
703-893-0600 / ggarrett@bdo.com

DOUGLAS HERMAN
Forensic Technology Services Principal
312-730-1260 / douglas.herman@bdo.com

JASON LIPSCHULTZ
Third Party Attestation Managing Director
312-616-3941 / jlipschultz@bdo.com