SHEARMAN & STERLING LLP

CLIENT PUBLICATION

PRIVACY & DATA PROTECTION | SEPTEMBER 30, 2016

Privacy and Cybersecurity Checklist When Designing a Family Office

As family office executives set up a family office or review an existing family office, it is important to make sure the privacy and cybersecurity concerns are addressed and the governance and information security infrastructures are set up to get it right from the start. Working with a family office means personalized and tailored services are delivered that take into consideration a family's entire situation, including their assets and liabilities, as well as wealth transfer, intergenerational and philanthropic objectives. Thus, protecting the privacy and confidentiality of not only the financial and wealth management decisions but also the personal information, goals and preferences of the underlying family are of utmost importance. Family offices can establish privacy and cybersecurity controls that proactively mitigate risks related to cyber attacks and implement incident response playbooks that help families plan ahead in the event of a breach.

There are two types of family offices – single-family and multi-family offices. Whether the family office manages the financial and personal affairs of one family or multiple families are sharing resources and infrastructure costs through a multi-family office, delivering products and services in investment advising, financial planning or tax planning means a great deal of sensitive personal information will be collected, processed and managed by family offices. Below are checklists to assist family offices in identifying data privacy and cybersecurity risks.

Know Your Data: How to Design a Critical Asset Protection Program

The first step to protecting the privacy and confidentiality of the most sensitive information housed by family offices is to know the data. By asking the who, what, when, where and how of what the family considers to be the most sensitive and critical asset, a family office can identify and design a critical asset protection program that is right-sized and risk-based. When designing a family office or reviewing an existing family office, consider the following:

- Who - Whose information is collected, processed and managed by the family office? Does it include multiple generations' data, including children's data for example, or is the data set limited to the family leaders?
- What - What types of data classification or access management controls are in place to ensure that only the right amount of data and personal information is used or processed by the family office?
- When - Are there repeated processes, regular schedules by which investment decisions or asset transfers are made, for example, which a malicious attacker or an insider could exploit?
- Where - If the family office has a presence overseas, or if it has clients overseas, what non-US laws might a family office need to comply with in terms of data transfer restrictions and other regulatory obligations?
- How - How is the data being used and for what purpose? Is the data being shared with any third parties, including service providers or other hosting services?

Protect Yourself From Cyber Attack, but Have a Plan (Just in Case)

Once a basic level of governance and infrastructure controls is put in place as described above, specific protocols can be implemented to meet the physical, technical and organizational needs in terms of cyber security risks. Hacking and other cyber attacks have occurred with increasing frequency, especially in the financial services sector, but the potential harm may be mitigated if an organization can deal with such incidents effectively. In preparing a response to a data breach, a family office may consider the following five core functions of a cybersecurity framework:

Five Core Functions of a Cybersecurity Framework

Identify	▪ *Have an understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities*. Have you considered specific kinds of cyber attacks? Different types of cyber attacks may demand different responses. A ransomware attack, for example, raises questions about backup policies, whether information is backed up thoroughly or held offline. Risk assessments should be conducted regularly to design and implement a comprehensive risk management strategy.
Protect	▪ *Controls and safeguard necessary to protect or deter cybersecurity threats*. Are controls in place and have employees been trained on those controls? Establishing access controls to sensitive information and training employees and service providers on the safeguards will help maintain a cybersecurity program that protects the organization from internal and external threats. To test the effectiveness of such controls and training, regularly-scheduled phishing tests or tabletop exercises are recommended to test how the organization fares in response to attacks and breaches.
Detect	▪ *Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events*. Are data forensic capabilities in place that will detect anomalies, fraud activities or data theft events? A robust data security program should include forensics and monitoring that will assist in not only detecting a cyber attack or a breach but also analyzing and understanding them after such vulnerability is discovered.
Respond	▪ *Incident-response activities*. Is an incident response team in place and does the team have a playbook to follow in the event of a breach? A cross-disciplinary team should be in place to receive reports, investigate potential breaches and to respond to known breaches. Response plans and playbooks should clarify roles and responsibilities, including how the family will be notified, whether law enforcement will be contacted and who will analyze various other legal requirements for notification that may be triggered.

Recover

- *Business continuity plans to maintain resilience and recover capabilities after a cyber breach*. If a severe cyberattack renders the family office's network unusable, how fast can the network be shut down and brought back into operation? Recovery planning should include not only procedures for how to best respond and keep the organization resilient but also how lessons learned from "near-misses" can be incorporated to address data security gaps and reduce future risks.

Key Takeaways:

- *Know your data*. Establishing a comprehensive data privacy and cybersecurity program can feel overwhelming. To begin the process of determining a risk-based approach, the first step should be to inventory the data and establishing basic governance and infrastructure controls, such as implementing policies and procedures to identify the critical assets handled and managed by the family office.
- *Have a plan*. No cyber security program will be 100% successful in detecting and preventing all cyber attacks and data thefts. Implement a cybersecurity framework that sets industry-standard levels of controls to identify, protect, detect, respond and recover from data breaches.

For more information, please contact the Shearman & Sterling Global Privacy and Data Protection practice.

CONTACTS

Jeewon Kim Serrato
Washington, DC
+1.202.508.8032
jeewon.serrato@shearman.com

Richard C. Hsu
Menlo Park
+1.650.838.3774
richard.hsu@shearman.com

Marc Elzweig
Menlo Park
+1.650.838.3815
marc.elzweig@shearman.com

599 LEXINGTON AVENUE | NEW YORK | NY | 10022-6069