2022 PRIORITIES MITIGATING FAMILY OFFICE CYBERSECURITY RISK

Over 50% of ultra-high net worth family wealth is being managed through family offices, yet even the largest family offices lack the security resources of most banks and large corporations. This makes them a huge target for cyber criminals, and cyber threats are becoming more pervasive for family offices of all sizes. Not surprisingly, cybersecurity is the number-one concern for Family Office Exchange (FOX) members, according to the 2021 FOX State of the Family Office Industry survey. Yet many family offices continue to operate without the proper tools to monitor and prevent cybersecurity attacks.

In this piece, we'll cover what family offices should be prioritizing in 2022 to mitigate cybersecurity risk.

WHY ARE FAMILY OFFICES AT RISK?

The US Family Office Club estimates that there are 500 to 1000 single-family offices in United States and around 2500 to 3000 multi-family offices that manage $300 billion+ in assets. With cyber threats becoming more widespread, cybersecurity should be a top priority for family offices. Below are some of the current cyber trends.

Current Cybersecurity Trends

$3.86 million is the average cost of a data breach globally

80% of breaches expose customer personal identifiable information (PII)

56% of organizations don't have a cyber incident response plan

Family offices have what cybercriminals want: valuable assets. However, many family offices can fall victim to cyber-attacks that are not financially motivated. Unlike other types of organizations, family offices are at higher risk of cyberattacks due to the potential for blackmail, extortion, and smear campaigns since they represent a tremendous amount of wealth from well-known, influential individuals.

Unpreparedness for COVID-19 has also put family offices at risk. Remote work is one of the biggest challenges for family offices. Not only does it put them at risk for more cybercriminal activity, but many family offices admit they wish they had better prepared their employees for remote work. Now more than ever, family offices should focus on cybersecurity and continue to improve their workforce's ability to work remotely.

BEST PRACTICES FOR MITIGATING RISK IN THE FAMILY OFFICE

As cybercrime evolves and cybercriminals become increasingly sophisticated in their attack methods, family offices must adapt. Just like any other organization, 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.

At the bare minimum, every family office should do the following three things:

Create and use strong passwords. Make sure that everyone within your organization knows what constitutes a good, strong password. No two passwords should ever be the same and they should always be complex. Use a password manager such as Dashlane to manage and secure your credentials.

Implement multi-factor authentication (MFA). MFA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence. It could be knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA can be quickly rolled out and will greatly increase security.

Use private networks. When employees use public Wi-Fi, they're putting sensitive company information at risk. Encourage team members to use private networks or other encryption solutions to secure communication. Additionally, you should always modify any default ID and password that ships with items such as Wi-Fi routers for your home or office. This guidance extends to anything you purchased such as home automation or digital assistants like Alexa. Hackers frequently attack default ID and passwords for products we don't think to secure.

Here are 7 additional tips for how family offices can stay secure and mitigate risk.

1. **Draft, Perfect, and Practice an Incident Response Plan**
   Having an incident response plan is one thing, putting it into practice and continuously questioning it is another. Every family office should have a document that outlines their approach when responding to incidents. The plan should include things like activities that happen in each phase, each person's responsibilities and how the plan supports the organization's mission. Once a plan is drawn up, put it into practice and continuously make revisions as you see fit.

2. **Have a Disaster Recovery Communication Process**
   Disaster recovery plans, unlike incident response plans, outline how an organization would resume normal operations after a disruption. A disruption could be anything from a cyberattack to a natural disaster to a simple equipment outage. How will your family office resume work in the event of an unforeseen disaster? Thinking about these scenarios ahead of time will ensure that you are fully prepared.

   A disaster recovery plan should do more than just outline how your organization plans to resume normal activities. It should clearly define who people should communicate with and how they should communicate with each other during distinct phases. If the communication process is not figured out ahead of time, an outage could be detrimental to your organization.

3. **Offer Continuing Education to Everyone**
   According to a study by Boston Private, only 58% of family offices have trained internal employees and their family members about risks. Offering continuing education should be a top priority for family offices. Often, your own employees can be the biggest threat to the organization. Offer continuing education to all professionals. Make sure they know what to look out for and are prepared for anything that may pose a threat to the organization.

4. **Test All Internal Employees with Cyber Incident Exercises**
   Take continuing education a step further by putting employees to the test. See if they can spot a cyber threat themselves. With realistic exercises, your employees can practice responding to cyber threats and be better prepared for whatever may come their way.

5. **Create a Culture of Awareness and Reporting**
   It's important to create a culture within the business that not only makes employees aware of cybersecurity but also encourages them to report incidents whenever they occur. Cybersecurity shouldn't just be a top priority among executives, it should be a part of the culture within your organization.

6. **Make Sure You Have Access to Robust and Timely Threat Data**
   Knowing how to respond to threats is important, but you must also effectively manage risk. This means having access to robust and timely threat data (i.e., the data that hackers and criminals seek the most). Family offices should have access to information about any significant risks that are affecting the business. The business should be constantly reviewing these to improve their security posture.

7. **Have Adequate Insurance Coverage**
   It shouldn't matter how confident you are in your security posture; every family office should still have insurance as a safety net. Insurance can afford financial protection should the worst-case scenario happen. The presence of insurance can also give peace of mind to the business owner as well as key stakeholders.

Every family office and high net worth individual needs to protect their valuable assets. This is why it's crucial that cybersecurity be a top priority. BDO Digital's **cybersecurity maturity quiz** gives you an idea of how secure your family office currently is. We also recommend speaking with a cyber specialist to discuss your organization's specific threat landscape in greater detail. **Contact us** today to get started.