September 7, 2022

Generations Summer 2022 - Keeping It in the Family: Ensuring the Confidentiality and Security of Family Member Information

Data privacy and cybersecurity are on everyone's mind these days. Ransomware, hacks, and data breaches are rampant, affecting all economic sectors and hundreds of millions of individuals each year. Many readers of this newsletter likely know this all too well after having a cybersecurity incident at their business or receiving a breach notification letter in the mail. The implications of these incidents can be significant and costly, ranging from the loss of highly sensitive personal information to extortion, cyber fraud, wire fraud, reputational risks, lawsuits, fines, penalties, and more. Family offices are not immune to this reality and in fact are often seen as soft targets for attack, given the information the family office holds on family members, the assets being managed, the frequency of fund transfers, and the relatively small size of many family offices. This combination puts them at particular risk. Why try to steal information from a Fortune 100 global bank when a smaller target with perhaps fewer defenses is available?

Cybersecurity Risks

Cybersecurity risks come in many forms, though a few are more pertinent to family offices. The cybersecurity risks discussed below are those most likely to affect a family office and the ones most likely to result in meaningful harm to family office members.

- *Ransomware*: A ransomware attack is one in which a cybercriminal infiltrates an organization's computer network, often as the result of a user clicking on an attachment or a link in a fraudulent email or the failure to secure the network properly against external parties. Once network access is obtained, the cybercriminal may lock the organization's files (preventing anyone other than the cybercriminal from accessing them) or steal copies of the organization's files and then threaten to publish them. In either instance, the cybercriminal may offer a sum of money (typically in cryptocurrency) that the organization could pay to regain access to its locked files or to prevent the files from being published. This extortion can be particularly dangerous for families of wealth, given the financial and reputational risks involved.
- *Cyber espionage*: Not every cybercriminal is after money—at least directly—from a family office. Some cybercriminals are more interested in learning about the family office's business plans, financial interests, strategies, and members. Other cybercriminals may be interested to learn where the children of family members attend boarding school or the flight schedule of a family member. As with ransomware, a cybercriminal will obtain access to the family office's computer network, but once access is obtained, the criminal will quietly go about collecting information for months (or even years). This information can then be sold to third parties seeking to block the family office's business dealings, media outlets looking to capitalize on an embarrassing or unfortunate incident, or financial criminals looking to siphon funds from the family office.
- *Masquerading*: A masquerading scheme is a type of cyber fraud in which the cybercriminal impersonates a family member or family office leader in order to trick a family office staff person into divulging confidential information or initiating a wire transfer to a fraudulent bank account. These frauds may be very sophisticated and often occur after months of studying both the target and the family member or other person being impersonated. The fraud often takes advantage of a change in operations or life events, such as parental leave or vacations. A successful masquerading scam can be devastating to a family office, resulting in the quick loss of significant funds or exposure of confidential information.

Best Practices

While cyber threats are prevalent and potentially very harmful to the family office and family members alike, there is quite a lot family office leaders can do to reduce the risk of an incident occurring and mitigate potential harms arising from an incident. The following best practices provide a road map for family office leaders looking to examine and improve their cybersecurity preparedness.

- *Understand applicable law*: Between federal and state laws, there are hundreds of data privacy and security laws on the books. Some of these laws apply to businesses and organizations generally, some to only specific sectors of the economy, and others in only certain limited contexts. These laws often govern how a business or organization may collect personal information and, once the business or organization possesses it, how the business or organization may use, retain, or re-disclose it. In light of this, it is vital for family offices to understand which laws they need to comply with, which laws they can safely ignore, and how to develop a compliance program to ensure the family office is satisfying applicable legal requirements. Examples of laws that may apply to family offices include laws protecting Social Security numbers, setting forth minimum cybersecurity protection standards, and outlining data breach response requirements. Family offices with members living abroad may also need to comply with the laws of those jurisdictions and other laws regarding the cross-border transfer of personal information. Compliance with these laws is the foundation of any cybersecurity and data protection program.
- *Information security review*: In collaboration with outside advisors, family offices should work to evaluate the sufficiency of the family office's current information security infrastructure (e.g., virus detection, firewalls, passwords). Based on the results of this review, a risk management plan should be created to identify opportunities for improvement, rank the opportunities by risk, and outline a process and timeline for implementing such improvements.
- *Incident response plan*: A family office should have in place a comprehensive incident response plan. This plan should outline how the family office intends to comply with applicable law, investigate an incident, bring in outside experts, notify affected family members, and take steps to protect family members from financial or reputational harm.
- *Have a team*: Complying with data privacy laws and ensuring data security are difficult for any organization, regardless of size or resources. To comply with the laws, protect family member data, and respond to a data security incident in a timely and appropriate manner, family offices should have a team of qualified advisors in place.

The laws and best practices described above are designed to safeguard family member information and reduce the likelihood of a data breach. Importantly, legal compliance and the adoption of best practices demonstrate that if a breach someday occurs, a well-prepared family office can act promptly and effectively in a manner consistent with the expectations of government regulators. Otherwise, a family office may be at much greater risk of government investigations, fines and penalties, and legal claims from family members. Since no family office can be absolutely breach-proof, all family offices should be breach-
ready.

Would you like to receive our *Day Pitney Generations Newsletter?* Sign up here. Day Pitney Generations Newsletter - Summer 2022 (pdf)

Authors



William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com



R. Scott Beach
Partner

Greenwich, CT | (203) 862-7824

Stamford, CT | (203) 977-7336

rsbeach@daypitney.com