28 May 2020

Family Offices: Cybersecurity Threats and Best Practices

The ongoing coronavirus pandemic has dramatically shifted work patterns for many family offices, increasing the degree to which employees are using IT infrastructure to communicate and analyze and complete deals. In addition, as the Federal Trade Commission and others have reported, cyber criminals appear to be more active than ever and are leveraging the pandemic through a variety of scams to steal money and information from businesses and individuals. As a result, it is a particularly opportune time for family offices of all sizes to assess their plans and capabilities to prevent, detect and remediate cybersecurity attacks.

This article provides a brief overview of common cybersecurity threats that family offices might encounter and best practices that family offices should consider implementing to prevent such threats. Please note that this article does not intend to provide a comprehensive overview of cybersecurity threats and best practices; please consult your cybersecurity services provider or counsel for more information.

Common Cybersecurity Threats

1. **Business Email Compromise —** The single most common type of attack across all industries involves a business email compromise ("BEC"). BEC events typically occur through phishing emails designed to induce an individual to click on a malicious link, open a malicious document, or otherwise trick the person into disclosing his or her credentials for logging into a corporate system, such as an email system. Once an attacker successfully gains access to a corporate email account, a variety of potential harms could occur, such as theft of data, fraudulent wire transfers, fake capital call notices and ransomware, among others.

2. **Targeting Personnel —** Cyber attackers often target finance and accounting personnel and executive assistants due to their access to key systems and information. For example, an attacker might impersonate a senior executive and email finance and accounting personnel to initiate a wire transfer. Alternatively, an attacker might direct phishing schemes at an assistant in an attempt to steal valuable information about a senior executive or to use the assistant's email account to direct other employees to execute a wire transfer purportedly on behalf of senior management.

3. **Diversion of Funds Flow —** Over the past year, we have seen an uptick in cybersecurity attacks relating to the funds flow process in investment transactions. For example, some attackers have sought to substitute their own bank account information for that of an investment target just before closing a transaction. In other instances, attackers have sought to divert funds from a target's customers during the run-up to a transaction.

Best Practices to Prevent or Mitigate Cybersecurity Threats

Technical Operational Measures

1. **Two-Factor Authentication —** One way that family offices can help prevent BEC events is to require employees to use two-factor authentication to log into family office systems, including email. Two-factor authentication requires an individual to input two pieces of

information in order to log in to a system. The most commonly used "factors" are a password followed by a code sent to an individual's phone. Although some individuals view two-factor authentication as burdensome, the process is quickly gaining traction as a standard component of cybersecurity defenses because it can help prevent a broad range of common cybersecurity attacks. In the past year, several of our clients held off on implementing two-factor authentication, only to quickly implement it after experiencing a cyberattack.

2. **Backup IT Systems —** Family offices should consider periodically backing up their IT systems and critical assets. Once backups are complete, they should be stored in a way such that they are not accessible from the family office's operating or production environment. Taking these actions might enable a family office to minimize potential damage from an attack.

3. **Securing Cloud-Based Services —** Using cloud-based services, such as file storage services, can help quickly and effectively operationalize a business. However, cloud-based services represent another way in which a family office's sensitive data could be accessed or stolen. Consequently, family offices cannot simply rely on the cloud provider to ensure security of a family office's data; instead, family offices must ensure that the security settings for the cloud-based services are appropriately configured.

4. **Interacting with Third-Party Vendors and New Contacts —** Family offices should use extra caution when interacting with new third-party vendors and other contacts and should verify the identity of these counterparties through trusted means, particularly when engaging in a transaction involving a funds flow. Moreover, family offices should also diligence counterparties to ensure that such persons have appropriate data protection systems and processes in place.

Developing a Cybersecurity Program

1. **Incident Response Plan —** In the event of a cybersecurity incident, family offices need to be prepared to effectively respond to the incident, which includes resuming business operations with minimal impact and demonstrating to investors, employees and other parties that the incident was resolved appropriately. Establishing an incident response plan, which outlines steps to take in the event of a cybersecurity attack, can help family offices accomplish these goals. A key step in developing an effective incident response plan involves identifying external "first responders," which may include legal counsel, a forensic IT specialist and a company's insurance carrier (if applicable). In addition, family offices that are registered investment advisers should also consider the SEC's cybersecurity guidance in developing an incident response plan.

2. **Training —** Another critical step in mitigating cybersecurity risk is to train personnel on preventing, recognizing and escalating cyberattacks. For example, family offices should train employees to recognize phishing emails and malicious links and documents. Family offices should consider a range of training options, such as live training (i.e., classroom setting), online training and phishing email tests, in which organizations send fake phishing emails to their employees to evaluate their employees' response. In particular, finance and accounting personnel, along with executive assistants, should be trained to exercise particular caution when opening emails or receiving financial directives via email. Phone or in-person verification of financial directives can help prevent losses to the family office.

3. **Insurance —** Family offices should consider obtaining cybersecurity insurance, which can cover the costs of responding to a cybersecurity attack, including the costs of investigating the attack (including counsel and forensic IT firm costs), the costs of remediating the IT environment, and fees or liability from lawsuits or claims resulting from a cybersecurity attack. Family offices should also consider whether existing insurance policies (e.g., property or business interruption policies) cover cybersecurity incidents. Family offices should be aware that failing to follow a cybersecurity insurance policy's specific procedures for notifying the carrier can preclude coverage for certain expenses that would otherwise be recoverable, such as fees for legal counsel or a forensic IT specialist.

If you have questions about the topics addressed in this *Private Investment & Family Office Insights*, please contact familyoffice@kirkland.com or one of the attorneys listed below.

Olivia Adendorff, P.C.
olivia.adendorff@kirkland.com
+1 214 972 1758

Jennifer Avery-Emani
jennifer.avery@kirkland.com
+1 312 862 2712

Richard H. Cunningham, P.C.
rich.cunningham@kirkland.com
+1 202 389 3119

Ryan D. Harris, P.C.
ryan.harris@kirkland.com
+1 312 862 6479

Nadia Murad
nadia.murad@kirkland.com
+1 212 909 3499

Sunil Shenoi
sunil.shenoi@kirkland.com
+1 312 862 3028

Seth Traxler, P.C.
seth.traxler@kirkland.com
+1 312 862 2241