GREENPOINT
ADVISORS

Private Wealth | May 2010 issue

Safeguarding Client Privacy

These are some of the steps family offices can take to secure their confidential client information.
By Jim Campbell

Do single-family offices have the technology to provide the privacy and confidentiality that families desire? The simple answer is, not likely.

To be fair to SFOs, however, it is important to explain why. Financial service organizations such as multi-family offices, banks and investment firms are also challenged in this regard. But these organizations usually have deeper staffing and more money to invest in technology. Additionally, these organizations are subject to regulations and oversight that force them to have stronger controls. SFOs are not subject to this level of scrutiny.

Many wealthy families establish single-family offices for both investment and non-investment services. Another key objective is to put various services under strict family control so financial and personal affairs can be managed in a professional and confidential manner. In a 2007 Wharton Global Family Alliance Study of 138 SFOs of $100 million or more in the U.S. and Europe, confidentiality was tied for second with conflict-free advice as an important benefit to family clients. Trans-generational wealth management services were the most important.

Why is protecting privacy and confidentiality such a challenge? In an open architecture environment, it is extremely difficult for any organization to control every potential point where a breach of privacy and confidentiality may occur. Some may suggest that the task is easier for SFOs since they support only a single client and have a smaller infrastructure. On the flip side, however, SFOs typically have fewer people and capital resources than larger organizations. A smaller infrastructure does not necessarily mean fewer key control points, although it could mean less activity through the same amount of control points.

Moreover, SFOs usually support multiple generations and family branches, each with its own set of relationships, needs and service requirements. This creates operating inconsistencies and additional complexity.

There are three key areas that SFOs must consider when determining if they are adequately protecting their client:

- External service providers
- Internal technology
- The workplace

External Service Providers

External service providers need access to private and confidential information in order to do their job. They, in turn, have their own third-party service providers to support various aspects of their business. Some of these firms may have overseas offices and/or outsource work to low-cost companies in countries such as India or the Philippines. A typical family office will have relationships with a dozen or more external service providers, including custodian banks, brokers, investment firms, CPA firms, law firms and technology companies. The more external service providers a family office has, the more magnified the challenge of protecting privacy and confidentiality.

For an SFO, managing and overseeing the activities of external services providers are key functions.

SFOs should be asking themselves this question: To what extent are our external service providers going to protect our privacy and confidentiality.

To assess the ability of a third-party provider to secure confidential information, here is what an SFO should look for:

1. A privacy statement. In accordance with the Gramm-Leach-Bliley Act of 1999, financial institutions are required to provide their clients with a statement that describes their privacy policy concerning the disclosure of non-public, private information (NPPI). The statement should describe how the organization will go about protecting your information and what they typically disclose to and require of their third-party providers.

2. Staff training. Find out what programs are in place to teach staff the importance of protecting client privacy.

3. E-mail encryption and communication protocols. What policies do your external service providers have in place to protect electronic information? Are you accessing or receiving account information in a secure manner? Who is following the chain of control over your client's private and confidential information?

4. Due diligence of vendors. Find out what your provider does in order to ensure that its vendors are operating in a sound and secure manner. If the vendors have your private information, you are entitled to know this.

5. Industry certifications. Does your service provider maintain any industry certifications that demonstrate, to an independent reviewer, that they are operating in a sound and secure manner?

6. References. Talk to other SFOs and industry colleagues that have had experiences with your service providers. Check with industry groups that rate service providers.

7. What do they outsource? Find out what tasks your service providers outsource and to whom they are outsourced. You will likely be surprised that your service provider has a number of other firms that have your private information.

Internal Technology

Internal technology, including computer hardware, software, the Internet and portable devices, requires extensive security measures to protect clients' privacy and confidentiality. These are the potential vulnerabilities that should be addressed:

1. Laptop/portable device security. Laptops, PDAs and cell phones all contain private and confidential information and these devices must be considered vital assets that need to be safeguarded. Consequently, all mobile devices should be password protected and security procedures should be in place in case a device is lost or stolen.

2. E-mail encryption policy. SFOs should have an e-mail policy in place that includes message encryption. Encryption software will convert sensitive information such as passwords, names, identification numbers and account numbers into "unintelligent information." This, together with good internal policy regarding the use of e-mail, will help protect a family's privacy and confidentiality.

3. Internet access policy. SFOs should have an Internet access policy in place that requires access only through an approved firewall and/or an approved Internet service provider. Financial transactions and other messages that include account numbers and other personal information should not be sent over the Internet unless they have first been encrypted. Software downloads over the Internet

should be for business-related needs from trusted, well-known business partners. Staff should be prohibited from downloading music, videos or other applications for personal use.

4. Data access and user rights. All internal and external access to an SFO's business applications and communications network must be controlled by the SFO and/or its hosting service provider. SFOs must consider where best to utilize both hardware/software security devices and encryption technology. Users should have access to only those systems and to specific data that is required to perform their duties. Staff members should be reminded to keep their passwords and IDs confidential.

5. Attacks on information technology systems. It's important to be able to identify and assess the seriousness of potential security system breaches. System logs should be in place and reviewed daily by SFOs and/or their hosting service.

6. Data backup. Some SFOs have data backup procedures that are inconsistent with protecting privacy and confidentiality. For example, SFOs may back up key data, but the backup disk or tape that contains private information may not be kept secure. It may be taken home by a staff member, where it can get lost, stolen or copied. SFOs should approach data backup in a more secure manner.
The Workplace

Protecting privacy and confidentiality in the workplace begins with people. Hiring practices and background and reference checks are important. Employees should also be trained to deal with security issues. SFOs are usually very selective when hiring new employees, but they need to go further when it comes to raising their employees' awareness about what to do to protect private and confidential information.

SFOs need to consider the following workplace controls:

1. General office security. SFOs should evaluate their office security, including staff, vendor and visitor access to both the general premises and specific areas of the office. It is important to limit access to areas of the office where private and confidential information is accessible.

2. Work area policy.
    - How are documents that contain sensitive information discarded?
    - Do printer and copier areas and conference rooms get cluttered with documents that contain sensitive information?
- Do employees keep passwords, account numbers and other sensitive information on Post-it notes taped to their PCs?
    - Are physical files kept under lock and key? Who has access?
    - Are electronic files restricted to only those individuals that need to know?
    - Is there a shredding policy?

3. Staff training. SFOs should have a written policy and an introductory training session for employees that clearly explain what the expectations are regarding the safeguarding of sensitive information.

Many of the recommendations highlighted above can be implemented by SFOs in a relatively simple manner. SFOs should evaluate their current level of security and determine what steps they may need to take in order to enhance their ability to protect the privacy and confidentiality of their family members.

Jim Campbell (jim.campbell@windwardadvisorygroup.com) is a partner at Windward Advisory Group, a family office technology consultant in Princeton, N.J.