Avoiding a Data Breach in Family Offices

By Andrew D. Campbell

Some data security disasters make news because they involve household names -- Target Stores, Sony Online Entertainment and Home Depot, among others. While other data breaches make headlines because they reveal embarrassing information -- *e.g.*, Ashley Madison.

But that does not mean that family run offices, which may be less well-known and/or possess "less interesting" data than hacking victims in the news, should get complacent. If hackers find their way into your network and steal or corrupt data, personal information may be exposed, and confidential business information or trade secrets may be made public. Repairing the damage — and your business's reputation — can be time-consuming and costly. As a result, family run offices need to be proactive in protecting their data and know what to do if a breach occurs.

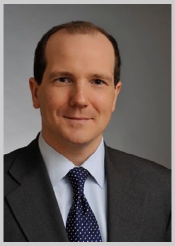
Repairing the damage — and your business's reputation — can be time-consuming and costly.

Among the most important steps any family office should take is to implement and follow data security policies and safeguards. There is not a comprehensive federal data-security law that applies to all industries (though some industries such as banking and health care are governed by federal laws), but many states have enacted statutes requiring all businesses that own or license personal information of the state's residents to adhere to certain standards. These standards can include:

- Designating an employee to maintain a comprehensive data security program;
- Identifying and assessing reasonably foreseeable internal and external risks to the security of data including:
  - ongoing employee training;
  - employee compliance with policies and procedures; and
  - means for detecting and preventing security system failures;
- Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises;
- Disciplining employees for violations of data security program rules;
- Overseeing service providers by, among other things;
  - Taking reasonable steps to select and retain third-party service providers who can maintain appropriate security measures to protect personal information; and
  - Requiring third-party service providers by contract to implement and maintain such appropriate security measures for personal information.
- Monitoring the security program to ensure it is operating in a manner reasonably calculated to prevent hacking and upgrading safeguards as necessary to limit risks; and
- Reviewing the scope of security measures annually, or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

As the above safeguards indicate, when it comes to data breaches an employee's conduct can be a significant source of vulnerability. Consistent with the above safeguards, a family office should train and consistently remind employees of the following:

- **Never open an unknown email attachment**. This should be obvious by now, but employees regularly open attachments and introduce viruses into company networks. Even email that appears to come from familiar sources could have been hijacked, so be cautious. As for attachments from strangers, delete them immediately without opening.



Fortune 500 companies, mid-size enterprises, start-ups and individuals all look to Andrew to help them resolve business disputes. These disputes arise out of, among other things, real estate transactions, equipment leases, consumer fraud claims, covenants not to compete, trade secrets claims and securities claims.

For more information about what to do if your company's sensitive data has been breached, contact:

Andrew D. Campbell
Novack and Macey LLP
acampbell@novackmacey.com or
(312) 419-6900

Avoiding a Data Breach in Family Offices

- **Regularly change passwords.** Don't give hackers time to figure out the passwords to your server and critical data. It may be a hassle to change passwords every 90 days, but do it anyway. Passwords should consist of a mix of upper and lower cases characters, numbers and special characters to add complexity and further reduce the risk of unauthorized entry.
- **Never leave passwords exposed.** Everyone has a co-worker who tapes his or her password to the computer monitor, but doing so invites trouble.
- **Turn off computers at night.** The easiest way to get past a password-protected server is to find a computer that's been left on after the user has gone home. The threat could come from a coworker who's using someone else's computer for illicit activity, or anyone with or without permission to access the premises after hours.
- **Communicate the importance of confidentiality.** Periodic breach avoidance training sessions help reinforce the importance of maintaining your company's privacy. It's not just electronic data that's at risk, either. The old-fashioned way of stealing secrets by rooting through trash cans or making off with carelessly stored files still works. If you don't need it, shred it. But first, check with your lawyers or accountants to make sure you aren't required to save the documents.

Portable devices used for work should be scanned periodically for malware and viruses, and employees should never install an unfamiliar jump drive or media device on a workplace computer.

But aside from attacks on your office computers, hackers can also access your data through portable devices. In a "bring your own device" world, employees merge work data onto personal tablets, laptops or other portable devices. Games and applications downloaded to personal devices from questionable sources can contain viruses or malware that infect workplace systems; they can also leak information stored on the portable device. To protect your data, make sure the workplace network is well protected from viruses and malware. Further, portable devices used for work should be scanned periodically for malware and viruses, and employees should never install an unfamiliar jump drive or media device on a workplace computer.

Employees using mobile devices in public Wi-Fi hotspots can also pose a danger, allowing hackers to intercept unencrypted data. Accordingly, employees should not use public Wi-Fi hotspots while communicating confidential information.

Finally, the physical loss of devices storing company information poses a significant risk. Accordingly, portable devices should be password protected and have a "kill pill" that will remotely wipe data from lost or stolen devices.

If, despite your best efforts, a data breach does occur, two people you should call are independent IT professionals and an attorney.

Independent IT professionals will provide you with a neutral assessment of the scope of the breach, how it happened and how it can be remedied. They can also aid in data retrieval, repairing corrupted files and getting your business back in operation. But, to get the most out of IT personnel, family offices need to back up their data regularly and often. Doing so will aid in getting your infected files and programs safely deleted and your system restored as soon as possible.

An attorney who specializes in litigation risk can help determine whether you are obligated to provide notice to individuals affected by the data breach and help you mitigate the potential damage from a breach. An attorney may also help you assess whether your losses may be covered by your insurance provider.

When it comes to a data breach, the best advice is to implement, monitor and update security measures and know where to turn if these measures fail.