

## Cyber Intrusion – Ready or Not

By Thomas DeMayo, Director, IT Risk Advisory

In today's cyber environment with all the news headlines focusing on the big data breaches and state-sponsored attacks, it is easy for family offices to avoid considering themselves as potential targets. In our presentations to, and discussions with, family offices, we find they continue to have this notion that they are too small and insignificant to be hacked. The truth of the situation is that they are the perfect targets, and cyber criminals are actively going after them.

Cyber criminals are very organized and business-oriented; they understand the fundamental concepts of risk vs. reward. Family offices and wealth advisors are typically smaller entities that have basic to weak cyber protections in-place making them easy to breach successfully, potentially yielding a large payout. We do not hear about these hacks in the news because very few victims are willing to openly discuss them.

### A Data Mine

So, what exactly is this payout? Family offices, by the nature of their business, have a cornucopia of personal and valuable information within their systems and under their control, including protected personal information, tax returns, bank and investment accounts, credit card numbers, health information, etc. These information assets can provide an attacker with many different channels of abuse, be it identity theft, balance transfers, or seeking ransom to not publicly disclose certain information.

### Not If, But When

Family offices need to take cyber threats seriously. It is not a matter of if but when a cyber security incident is going to occur in your family office. While trying to avoid becoming a victim and warding off the attackers might feel like a helpless situation, there are some very simple and inexpensive practices that a family office should be performing to give them a fighting chance.

More often than not, attackers will look at the economics of how much time and resources they want to invest in compromising your system. If you implement the basics and increase the level of difficulty, they will often abort and go to the family office down the block without protection that will yield the same payout.

### Cyber Security Best Practices

Some best practice considerations that all family offices and wealth advisors should follow are:

- Have an independent cyber security specialist perform an assessment to uncover risks as they relate to the people, processes and technology that make up the overall cyber program.
- Develop and maintain an information security framework.
- Provide security awareness training to all employees and to the family.

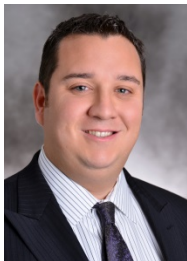
- This is especially important for the children who are often a prime source of targeting on social media because of the amount of information they disclose and their sometime willingness to interact with strangers.
- Perform phishing tests involving family office employees and family members to see who is prone to clicking or opening attachments in e-mails.
- Encrypt highly sensitive data at rest and in transit.
- Ensure mobile devices, such as smart phones and tablets, are adequately secured with a strong password, idle period time out, security software (if applicable), and encryption.
- If using cloud providers or outsourced IT contractors, ensure you have done adequate due diligence on how well they can safeguard the data with which they will be entrusted.

## Parting Words

You can either be proactive in securing your data systems or roll the dice by doing nothing. Right now, this is your choice.

\*\*\*

If you have any questions about the article, or would like a consultation regarding your organization's information security practices, please contact Tom DeMayo at [tdemayo@odpkf.com](mailto:tdemayo@odpkf.com) or 646.449.6353.



Thomas DeMayo  
CISSP, CIPP/US, CPT, CEH, CHFI, MCSE  
Director, IT Risk Advisory  
646.449.6353  
[tdemayo@odpkf.com](mailto:tdemayo@odpkf.com)

## About O'Connor Davies

O'Connor Davies, LLP is a full-service certified public accounting and advisory firm that has a long history of serving clients both domestically and internationally and providing specialized professional services of the highest quality. With roots tracing to 1891, nine offices located in New York, New Jersey, Connecticut and Maryland, and approximately 600 professionals, the Firm provides a complete range of audit, tax and advisory services. O'Connor Davies is ranked the 29th largest accounting firm in the country by *INSIDE Public Accounting* and the sixth largest in the Mid-Atlantic region by *Accounting Today*.

O'Connor Davies, LLP is a member firm of the PKF International Limited network of legally independent firms and does not accept any responsibility or liability for the actions or inactions on the part of any other individual member firm or firms.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.