Cybercrime: Rethinking Estate Planning and Asset Protection for Family Offices, High Net Worth Families and Executives

Michael S. Arlein and Craig A. Newman

As cybercrime has moved from the shadows to the center stage of consumer, corporate and national consciousness over the last decade, family offices, high net worth investors and individuals, executives and entrepreneurs have become prime targets of increasingly aggressive attacks.

The horror stories are all too common. The CFO of a multi-family office was waiting for his flight in an airport lounge when his laptop computer containing unencrypted client data was stolen. Within days, more than 180 clients became victims of identity theft and the multi-family office was forced into bankruptcy protection to fend off client lawsuits. Then there was the New York couple who unwittingly wired a $1.9 million deposit for their new co-op directly to cybercrminials that hacked into an email account, learned about the purchase, and created a bogus email and wire transfer instructions. In another case, a cybercriminal gathered enough personal data about a billionaire investor – mostly through social media channels – that he was able to call a private bank and provide sufficient identity-verifying information to open a credit card account outside the U.S. for a nonexistent "nephew."

Cybersecurity risk no doubt creates a vexing set of challenges for family offices, high net worth families and executives, who, like any other business, would be well-served to make cybersecurity an important part of their estate planning and asset protection strategies. In fact, a recent study by Morgan Stanley found that cybersecurity risk was at the top of the "worry list" for high net worth investors. The study asked high net worth investors which of the following issues they were most concerned about: terrorism, data security, or a major illness. Seventy-two percent of those surveyed ranked data security as their top concern, followed by terrorism and then a major illness.

The study covered high net worth individuals between the ages of 25 and 75, the majority of whom already had been victimized by cybercrime. Fifty-six percent have had data compromised by malware or a computer virus and forty percent have had their credit or debit card information stolen. Eight-percent of respondents said that their financial accounts had been hacked or compromised.

Even more telling, almost sixty percent of investors surveyed were concerned that they would be victimized by cybercrime "without even realizing it," and eighty-one percent said it was "difficult knowing how to protect [themselves] from identity theft with technology changing so quickly."

One of the most common cyber threats to family offices and high net worth families is "business email compromise," essentially spoof emails that very closely mimic a legitimate email, but seek to illegally transfer funds to a foreign bank account held by cybercriminals. Once the funds leave the family office or investor's account, they are nearly impossible to recover. In one case last year, cybercriminals made off with nearly $50 million by convincing an organization's finance department to transfer funds to a Hong Kong account belonging to the criminals. This scam has become so widespread that the FBI has issued private sector alerts to warn of this criminal activity.

Two other forms of cybercrime have become increasingly common: account takeover and ransomware. An account takeover involves stealing an investor's credentials for a financial account that can be accessed online. The most common method of doing so is through the use of malware that infects a computer – usually from an email attachment or link. The malware installs key logging software on the computer which allows the criminal to copy the user's credentials as they log into the financial institution's web site. Even token-generated passwords are vulnerable to this scam. The hacker then tries to move the account to another

[Reprinted with permission from Family Office Exchange, November 2016.]

institution before draining all of its assets. While the financial institutions generally reimburse the client for this kind of fraud, the financial losses are only the beginning. Aside from the time and energy required to clean up after an identity theft – from changing accounts to credit monitoring – once scammed, the victim's private details are often posted on a "suckers list" for other cybercriminals to victimize.

Then there is ransomware – essentially digital extortion – a high volume, high profit enterprise for cybercriminals. In a typical case, a criminal encrypts the victim's files, takes control of their computer or network and demands a ransom, usually in bitcoins to protect the criminal's identity. The victim is faced with the unenviable choice of taking the proverbial high road and not paying, or making the payment and hoping that it won't happen again.

While there are the obvious precautions for family offices and high net worth families and executives, such as keeping operating systems and software up to date and being careful with the use (and safe-keeping) of passwords, off-the-shelf solutions are not enough when investment assets are more sophisticated and global in nature, making them attractive targets for cybercriminals. If the family or executive is prominent, a host of other issues related to privacy and identity protection apply.

Here are a few steps for family offices, high net worth families and executives to consider, with the caveat that there is no one-size-fits-all approach:

- Conduct a comprehensive cyber vulnerability analysis, including an inventory of investment assets, custody arrangements, access control and general information, and asset security;

- Review data security precautions that asset managers, financial institutions and other investment advisers implement, making sure that investment agreements and customer documents, including those of third-party providers that might have access to your data or assets, provide appropriate safeguards;

- Examine risk of loss provisions in these agreements including liability in the event of a data breach;

- Ensure that your financial institutions, investment advisers and broker-dealers comply with governing data security regulations and consider enhanced internal controls and protections, especially for substantial asset transfers;

- Think through other data security vulnerabilities such as mobile applications and the security of your network, including wireless access;

- Consider consulting outside experts as resources permit; and,

- Review insurance policies and consider cyber, crime or fraud coverage when necessary.

While there is no simple solution to the growing risks posed by cybercrime, doing nothing is no longer an option.

Michael S. Arlein and Craig A. Newman are partners with Patterson Belknap Webb & Tyler LLP in New York. Mr. Arlein chairs the firm's Trusts & Estates Group and Mr. Newman chairs the firm's Privacy & Data Security Group.