SQUIRE PATTON BOGGS

Family Office Insights

The Growing Cyberthreat to Family Offices

Sophisticated cyberattacks are increasingly targeting family offices and ultrahigh net worth individuals. High net worth families and family offices can make attractive targets, as many lack sophisticated – or even basic – security infrastructure, and the global reach of some family offices can make the effects of a cyberattack even more devastating.

Ransomware is a type of software that locks a computer or network and sends a message to the affected users, refusing to release the affected devices until a ransom is paid. The most common types of ransomware encrypt the data stored on the network; that encryption can only be undone by the use of a unique computer code "key," which the perpetrators provide after being paid a ransom (usually in cryptocurrency, such as Bitcoin). Sometimes ransomware perpetrators, known as "threat actors" in the law enforcement and legal communities, will remove data from the affected systems before encrypting it and threaten to release it publicly or sell it on the dark web unless the ransom is paid. Oftentimes, this data has been specifically sought out and stolen by the threat actors well before the computer systems are locked and the ransom demanded – sometimes months before. This is clear evidence of the sophistication and planning behind these crimes.

Family offices and high net worth individuals are prime targets for ransomware for several reasons. The first is their frequent lack of the kinds of sophisticated information security that major corporations often employ. Although family offices may not initially believe they have data that would present a tempting target for cybercriminals, they often have financial information that would cause major problems if revealed publicly or sold to criminals. Beyond that, criminals might search for potentially embarrassing or private information about the individual or family – especially if the computers or networks are used for both personal and office business – and demand a ransom not to publicize such information.

"Phishing" is a form of cybercrime that gets its name from the way in which the criminals set out "bait" (often in the form of faked or spoofed emails) and hope someone clicks on a link or follows instructions they should not. The user then gets "caught," infecting their network. Some phishing emails are generic and might imitate a communication from a common internet provider or retailer; the malicious link might simply download a virus onto the computer of the person who clicked on it. Links could, however, lead to a spoofed webpage or website, which tries to trick unwary users into entering credit card or banking information.

"Spear-phishing" is more targeted: a threat actor sends a specific, fake email, often with sophisticated masking or spoofing to make it appear to come from a familiar person at their usual email address. Sometimes the actors have infiltrated the email systems of a target long before they launch the attack and have read and studied the language and diction of the person they are trying to imitate. They will include personal details gleaned from earlier communications and discuss imminent transactions in order to supply fake wiring or routing instructions. Such attacks have successfully stolen hundreds of millions of dollars in recent years. It is easy to see how family offices and high net worth individuals would be attractive targets for sophisticated spear-phishing attacks, since their operations often follow fewer bureaucratic procedures, and can be subject to fewer internal verification checks, than are common in the corporate world.

Possible Repercussions and Cross-border Complexities

Some of the repercussions from ransomware and spear-phishing attacks are obvious. For ransomware, if you choose not to pay the ransom (and sometimes even if you do), your computer systems may not be functional for days and the data that was encrypted may be damaged or destroyed even if it is restored. Ransoms can run into the millions of dollars, depending on the size of the attack and the value of the target – and to pay them, you first need to secure some Bitcoin. There are also specific problems relating to global issues: ransomware is almost always a cross-border crime. The computer programs that enable ransomware attacks are bought and sold by criminals on the black market online and the perpetrators themselves are often located in unfriendly jurisdictions. The FBI (in the US) and Europol (in the EU) are acutely aware of the growing tide of ransomware and, while they can be helpful in resolving some attacks, the ability of any law enforcement agency to reach these threat actors in person is limited not just by the internet-based nature of the crimes, but also by the difficulty of asserting jurisdiction in many of the countries where the threat actors choose to locate.

That same issue makes payment of ransoms tricky as well. In the US, many threat actors and developers of ransomware have been "designated" by the Treasury Department's Office of Foreign Asset Control (OFAC). This means that US citizens or businesses may not have dealings with them – and that includes paying ransomware ransoms. OFAC has specifically warned against paying ransoms, without making sure the money is not going to a designated group or person, and it is almost impossible to tell where the proceeds of a cryptocurrency transaction are actually headed.

Spear-phishing transactions may similarly entangle family offices in complicated cross-border problems. In addition to jurisdictional problems for law enforcement, once money has been transferred by wire, it can be extremely difficult to prove that the transfer was unintentional or caused by malicious action and to retrieve the money after the transfer has been made. The bank accounts used by threat actors in spear-phishing attacks are almost always outside of the victim's home country and, unsurprisingly, the money is usually moved out of the initial account immediately. Even if the money can be traced, working with international regulators to prove the nature of the transfer and reverse the ill-gotten gains can be a daunting prospect.

Ways to Protect Yourself

Whether the victim is a Fortune 100 corporation or a family office, there is a common element in most cyberattacks: human error. The easiest way to get into a castle, after all, is not to break down the walls, but to trick someone on the inside into opening the gate for you. Ransomware may be introduced into a computer network by "hacking" or other computer-based means, but often it is introduced via phishing emails containing malicious links. Those require a person to mistakenly click on a link. While adding network and device security is crucial for all organizations, training all the users of a computer network on how to identify and avoid cyberattacks like phishing is even more crucial. For family offices and high net worth individuals, that means everyone who has access to the family's or family office's computers or computer network needs to be aware of the threat of cyberattacks and have an understanding of how to minimize the risk of a successful cyberattack. Training tools are widely available and, thankfully, such training is far less expensive than the kinds of security software and hardware used by large corporations. Other basic but crucial activities include updating software – especially operating systems like Windows – on a regular basis, controlling and updating who has access to devices and networks, and continuously monitoring and improving the physical security and data security of the family office. One of the biggest dangers for any organization is the tendency to treat data security as a "one-and-done" problem, and to assume that the implementation of a solution at one point in time will solve the related problem into the indefinite future. Data security threats evolve constantly, and family offices and high net worth individuals must be vigilant, informed and adaptable as well.

Contacts

Daniel G. Berick
Partner, Cleveland
T +1 216 479 8374
E daniel.berick@squirepb.com

J.D. Bridges
Associate, Cleveland
T +1 216 479 8581
E jd.bridges@squirepb.com