Cyber Security Concerns and the High Net-Worth Family Office

The digitally interconnected nature of our society extends throughout the range of human activities, spanning social communication, family member interaction, business networking, education, financial transactions, medical care and travel. Moreover, these information exchanges are now proliferating across mobile networks, and highly private information is managed and moved across the internet by a diverse cast of characters (banks, telecommunications companies, media conglomerates, technology firms, etc.). The intersection of these layers of "connectedness" each represents a potential point of vulnerability. Many of these vulnerabilities can be mitigated by changes in user behavior. These changes have to be based on an understanding of how your behavior makes a difference.

Protecting and Educating Minors

Educating your family members and your staff on how their digital decisions affect the family's virtual and physical security is critical. High net-worth families may have a higher public profile to begin with, and represent an interesting news subject for a content hungry public. This means that your information will be more likely to be sought after than the average internet user. Education must include younger family members as well. Children are less aware of the potential dangers of over sharing information and more influenced by peers who encourage such decisions for social reasons. Even mature teens can fail to understand the very real risks of sharing personal information via social media (see sidebar).

One fifth of all registered Facebook accounts belong to people under the age of 17. Children are passionate about networking and rarely consider the dangers of over sharing family information. Additionally, poor understanding of privacy settings, and the desire to compete socially can lead to bad decisions about online personal conduct. This avenue of family data is specifically targeted by cyber stalkers who rely on the digital garrulity of children to obtain personal information for a variety of potentially criminal purposes, ranging from sexual predation, bullying, extortion, kidnap or financial data. Changing the way minors think about their online behavior has to happen deliberately, and education is one component. Monitoring online behavior is also beneficial, and can be negotiated with your family.

Location Based Services Can Be A Special Hazard

The proliferation of Global Positioning Services (GPS) technology in our personal and business devices offers tremendous advantages. It also is a source of great vulnerability. This can manifest in a variety of ways. Two of the most serious for potential cyber stalking are social media games and digital pictures. Social media games which encourage "check in's", track the physical behavior of family members who "like" cafes, movie theaters, schools, malls etc. Pictures taken with modern devices include special, hidden information (called EXIF data) which records the date, time, location, device type etc. allowing the possessor of the image to easily track the subject. Staff and family members need to be aware that they are participating in games and that images which they post should be first scrubbed of EXIF data.

In April 2011, Ivan Kaspersky, son of the multi-millionaire founder of Russian internet security firm Kaspersky Software, was kidnapped and held for five days before being rescued by Special Forces and police. A college student, he was abducted while commuting to his internship at a technology company. Ivan was very active in social media, and subsequent debriefing of his captors revealed that he was targeted due to the combination of his father's wealth and the readily available detailed information about his routine and his family posted by Ivan in social medial site Vkontakte.

Source: Evgeny Kaspersky, May 2011

Staff and Business Processes Create Vulnerabilities

"On the go" families rely on their staff for variety of services, from routine chores to extended travel support to reconciling financial transactions. These kinds of services often have an online component that can ease complexity or increase the business flexibility for the family. As the use of these services increases, the desire for even greater speed and convenience may lead to inadvertent information disclosure since each service provider hosts a small portion of your "family picture". It is important that the family office consistently conceal the identity of its principals where ever possible when establishing or using internet conveniences (dry cleaning, ticket booking, limousine service, etc.). Staff should be trained in this requirement, and the relevant family office business policy should be periodically audited.

Factbox: 10 ways to protect your family and staff online

1. Educate your family, especially minor children, on the importance of keeping personal and "family matters" OFF social networks.
2. Never post anything online which can be used to locate your family members or staff. Keep your routines private.
3. The internet has an infinite memory. Never post something which may be a source of future liability – when unsure, DO NOT post it.
4. Monitor the office and home networks to detect misuse or unintentionally dangerous behavior.
5. The family identity should be obfuscated when using digitally enabled conveniences, even when business is conducted via staff or other proxy.
6. Practice good internet hygiene by avoiding sites known to launch malware attacks. Be skeptical of email links and file sharing — follow up by phone or text when unsure.
7. Staff and family members should be educated on the potential risks of participating in location based social media.
8. Digital pictures which are posted online must be "cleaned" of hidden location, time and device information.
9. Security and usability are a compromise; find the right balance for your family.
10. Online risks are here to stay – make your response flexible but sustainable.

Vulnerabilities can be exploited in a number of ways. Family offices which permit employees to use their own devices to conduct family business apart from voice calls, or to be responsible for managing the configuration of family issued mobile PCs and phones are further at risk. This is because high net-worth families can be specifically targeted for internet enabled fraud schemes. "Spear phishing", or the application of highly tailored fraudulent communications, can appear to come from trusted members of the family network and can be hard to detect, especially by staff members who do not have first-hand acquaintance with the misrepresented person or company.

Mitigating online, targeted fraud requires family and staff education. All staff and adult family members should have a basic understanding of how common fraud schemes work. Fundamental online hygiene should be taught and followed, from avoiding certain categories of websites, (gambling, adult sites and related sites) to never clicking on links sent via email. When in doubt, it is much safer to call or text your contact to see if the linked information is legitimate. All of the internet devices used by staff and family should have up to date protections, and include precautions such as screen locks, remote tracking and data destruction capabilities (in the event of loss).

Balance Access and Protection

Every family is different, and there is no one size fits all solution. This article, intended for the principals and family office managers, is intended to plainly communicate some risks relating to cyber security. However, the benefits and pleasures of online interaction are valuable, so each family and office can find their uniquely tailored answer. As Evgeny Kaspersky, father of the kidnapped teen, said after his son was recovered, find ways to minimize risks instead of prompting minors to ignore guidelines — "Make your kids play the privacy game and be proud of protecting their family and their future."

Article contributed by Michael Massa of Torchstone Global. Michael consults for Torchstone Global, which discreetly serves world leading individuals, families and organizations with end-to-end risk avoidance solutions. TorchStone provides strategic security advisory services to the world-wide affluent community. For more information, please visit www.torchstoneglobal.com