Family Office Risk Management in the Digital World

In North America alone, over 4,500 family offices provide wealth management for, and oversee the affairs of, ultra-high net worth families. Family offices differ as widely in form and function as the families they represent. However, there are many commonalities among the challenges they face and the roles they fill, including family office risk management.

Many family offices manage wealth equivalent to that of a small or mid-size business (SMB), and they face similar technology needs. As in an SMB, family office technology must provide the basic infrastructure for communication and document management in a safe and secure environment.

Unique Risks

At the same time, the distinctive circumstances of a family office add an additional layer of complexity. Cyber-crime threatens not only the financial well-being of the family, but also the personal safety and reputation of family members. Some of the unique conditions include:

- **Limited staff** – While family offices manage finances similar in scope to a SMB, they often do so with a much smaller staff. This can result in a lack of in-house technology expertise and reduced levels of security. Families can become attractive targets for cyber-crime.

- **Out-of-date systems** – Unless the family office includes dedicated technology expertise or contracts with a managed services provider, systems quickly fall out-of-date. This makes networks vulnerable to hackers.
- **Multi-generational families** – Once a family reaches the third generation and beyond, family members are often spread out over various cities and countries. Family offices must facilitate remote access and communication in a way that is fully secure and adaptable to the variable circumstances of family members.

Human Element

In any organization, the weakest links in the security chain are the people. A typical family office employs fewer than ten staff members, and these employees may have far-reaching access to personal and financial data. They often work odd hours and need to address requests and concerns quickly and privately.

Hackers routinely use social engineering and email to great effect. An employee who clicks on a malicious file or responds to a request from a seemingly legitimate source may give hackers instant access to sensitive information, a serious family office risk management concern.

Benefits and Risks of the Cloud

The family office manages large amounts of data and facilitates communication among staff and family members in a wide variety of locations. The cloud offers powerful solutions for content management and remote access needs.

With documents stored in the cloud, family members and employees can access critical information and communicate via mobile technology from virtually anywhere in the world. This remote access provides necessary flexibility. At the same time, it also increases the vulnerabilities that the family office risk management strategy must address.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
hp Partner of the Year
ShoreTel Sky Partner of the Year

Family Office Risk Management Strategies

As with any business, family offices must employ a multi-faceted strategy to mitigate cyber-security risks. Key components of this strategy should include:

- **Inventory of connected equipment** – Conduct yearly inventories of everything connected to the internet. Ensure that all devices have updated software, robust passwords, and virus protection. This includes obvious items like laptops, routers and tablets. Also, check all smart devices such as printers and security cameras.
- **Secure access points** – Replace routers every few years. Emphasize the dangers of public Wi-Fi usage, and strengthen email protection.
- **Strategies to address the human factor** – Education is key. Create cyber-security policies surrounding passwords, connected devices, social media, payment authorization, email and so forth. Train office staff and family members regarding security policies. Implement access control measures to allow users only the access they need.
- **Layered security** – Virus protection alone will not provide adequate defense from attack. Implement a layered approach that combines attack prevention with detection and response. Employ available technology tools for encryption, backups, vulnerability testing and monitoring.

Benefits of a Trusted Partner

Implementing the right technology in the right way can ensure security and privacy of critical information and provide the flexibility to adapt to changing circumstances. Choosing a trusted technology services provider eases the burden on the family office, allowing staff to focus on wealth management, philanthropic initiatives and other priorities.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
hp Partner of the Year
ShoreTel Sky Partner of the Year