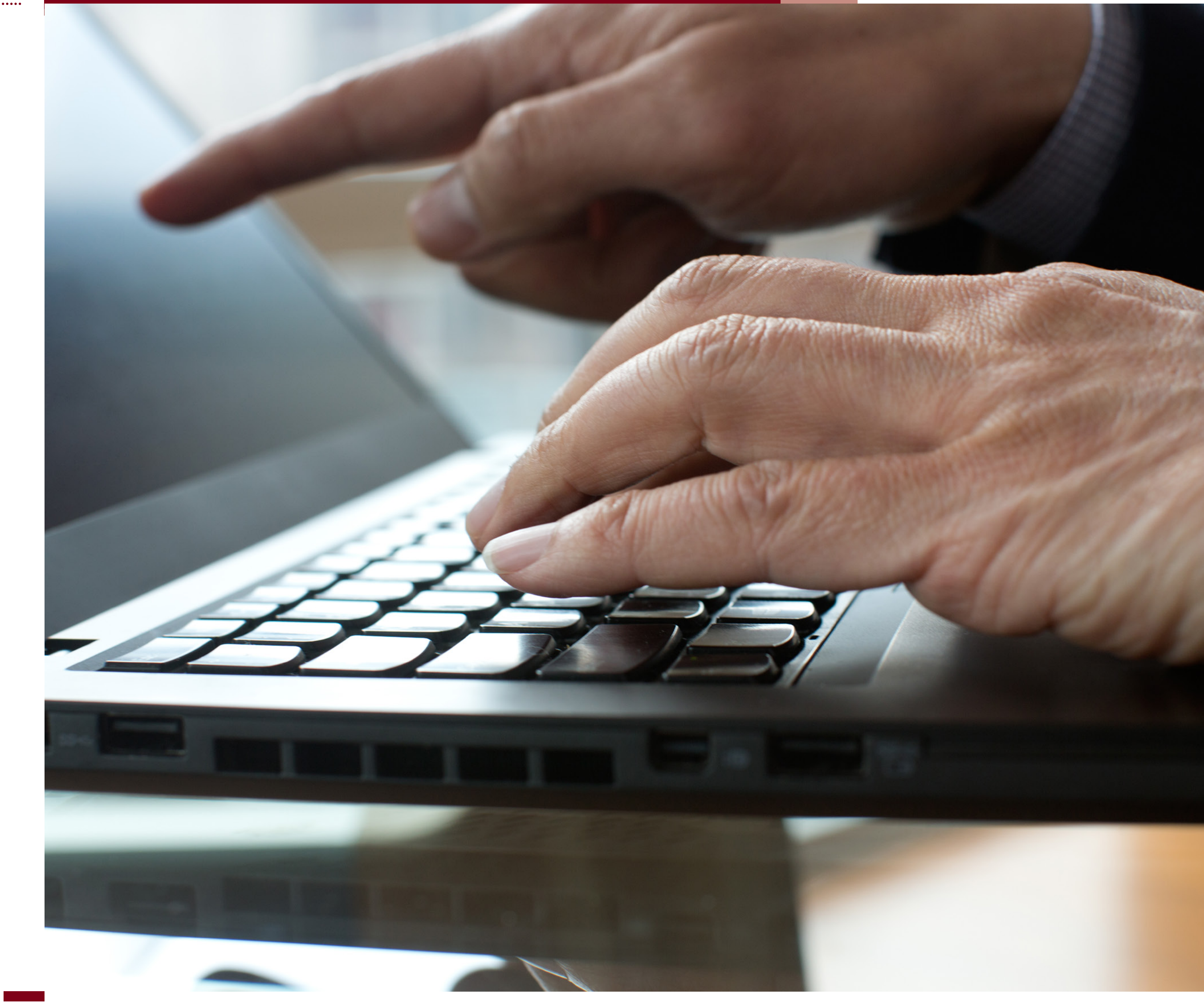
Creating an effective cyber-protection plan for your family office

It is possible to manage cyber risks while taking full advantage of digital technology.



The internet and connected devices are transforming the world, mostly for the better -- but for all the advantages cyberspace brings, there are also growing risks for businesses and families, all of which are relevant for family offices. Unfortunately, no organization or individual is immune to cyber risks. Staying out of the limelight is no silver bullet and can create a false sense of security. We've worked with families who say they are fully disconnected from the internet and still managed to find severe digital vulnerabilities.

We're all vulnerable[1] -- but wealthy families are particularly attractive targets in the eyes of cybercriminals. Willie Sutton said it best back in 1951, "I rob banks because that's where the money is." In addition, family offices are often unaware just how much of their personal information is publicly available. This can be surprising to families accustomed to taking proactive steps offline to stay under the radar. It is easier than many realize for fraudsters to piece together disparate data points, steal identities and launch sophisticated, criminal schemes in cyberspace. Further, over-reliance on communications providers and device makers to provide adequate protection can lead many families to forgo even the most basic protective steps. Family offices can also be vulnerable to cybercrime because of their interest in early adoption of leading-edge technologies - including connected devices - which may not have been subject in development to the sort of testing needed to enable robust protections for cybersecurity and privacy. In fact, many such devices are not designed with such protections in mind.

Managing the risk before trouble strikes

During 2017, the WannaCry ransomware outbreak in May and the Petya cyberattack in June reinforced a view that we at PwC have promoted for a long time: Effective protection against cyberattacks has less to do with any particular technological factor, and everything to do with proactive risk management in general.[2]

The WannaCry attack spread to 150 countries over a few days in May 2017 in part because it infected computers where users did not install a patch from Microsoft that was issued a few months earlier. The Petya cyberattack exploited the same vulnerability.

As these attacks show, robust cyber hygiene is a front-line defense. We recommend that family offices create a strategic plan to address the various types of cyber threats, and continually review and update that plan as new threats emerge. This action plan is designed to manage cyber risks by enabling smarter use of digital technology. Let's begin:

[1] "AICPA Survey: One-in-four Americans Victimized by Information Security Breaches," AICPA, 4/21/2015

[2] "Cybersecurity after WannaCry: How to Resist Future Attacks," David Burg and Sean Joyce, Strategy+ Business, 5/16/2017

Seven sides of a robust cyber policy, designed to cover a family office

1 *Maintain an updated inventory of everything that the family and the office use to connect to the internet, while in the office and beyond.*

Laptops, smartphones, tablets, routers and connected devices ranging from printers to refrigerators to cars can provide access points for cybercriminals. We encourage family offices to review each device at least once a year against the following questions:

- Is password protection enabled for each device?
- Is there virus protection and a firewall installed on each device, whether in the office or at home?
- Is the software current and routinely updated on each device?

Smartphones by themselves are not typically a frequent source of vulnerability, assuming password protection is activated, the software is current and they aren't used over public Wi-Fi. However, thieves can use inexpensive tools to monitor and listen to calls.[3] If family members are using phones in certain foreign countries, or if they are actively involved in confidential business dealings that may be targeted, then they should consider encrypted phone services.

2 *Assert control over internet access points, inside the office and beyond.*

Public Wi-Fi is one of the most common sources of breaches. When a family member logs into their email from open wireless access systems often used in coffee shops or hotels, thieves can intercept passwords as they are typed, along with pictures and data stored on the device. Many security experts tell families to not use public Wi-Fi under any circumstances. However, there are times where data service is not available or perhaps too slow. Using a Virtual Private Network (VPN) on top of the Wi-Fi is a relatively inexpensive solution that significantly increases protection.

Home and office routers are other points of vulnerability.[4] Routers are often used beyond their "end of life," or the time where manufacturers stop issuing software updates for them. Here's a basic checklist to follow to improve security related to routers. Ensure the routers:

- Have current software;
- Are replaced every few years; and
- Are password enabled and use robust passwords.

Also, ensure that remote administration is turned off and that the routers themselves are "non-discoverable" (this means that the router won't automatically appear in your network listing; the user has to know the name of the network as well as the password).

[3] "Privacy hawks in Congress call on Homeland Security to warn Americans of SS7 hacking threat," Taylor Hatmaker, TechCrunch, 3/15/2017

[4] "Rarely Patched Software Bugs in Home Routers Cripple Security," Jennifer Valentino-DeVries, Wall Street Journal, 1/18/2016

What is … Ransomware?

A virus typically spread by a corrupted link in an email. Once A PC is infected, victims are unable to access their data until a ransom is paid.

Research conducted by PwC found that most ransomware incidents resulted in hours of downtime or networks taken offline for up to 10 days. Moreover, the attackers still hold any proprietary data they picked up.

Ransom, blackmail, surveillance, shutdown, and data manipulation are all more feasible than they were only a few months ago.

The techniques and exploits used to distribute the WannaCry attack were only recently leaked to the world in April 2017.

Cybersecurity after WannaCry: How to Resist Future Attacks
PwC's Strategy & Business

3 *Write down (and review together) your Cybersecurity Policies*

Family offices should have a series of written cybersecurity policies, providing guidance to family and staff. Although there are few good ways to enforce such policies, writing them down and reviewing them at family meetings substantially increases compliance rates. Such policies often include the following:

- ***Connected device policy:*** This describes use of public Wi-Fi, VPNs and home routers.
- ***Identity protection policy:*** This describes how the family office protects the personal identity of each family member. Often, family offices provide credit monitoring service for each family member, perhaps even freezing their credit so that new accounts can't be opened without separate approval.
- ***Social media policy:*** This explains how family members use social media. The policy covers items that protect the physical security of the family, maintain private information, and protect the image and reputation of the family and business.
- ***Password policy:*** This describes what the family decides is a reasonable standard for passwords, on phones, tablets, routers and similar devices. This policy may include having the family office cover the cost of using a password utility for managing and simplifying password use.
- ***Payment-authorization policy:*** This is similar to how a bank approves wires or other payments. Recent years have seen high volumes of family emails being hacked into, with thieves copying family member language and style to send requests (purportedly from the family member) for wire transfers.

4 *Proactively address the people risks*

A robust cybersecurity strategy also must take into account the human side of the equation. Insiders – think of suppliers, vendors and employees – can create major risks either by accident or on purpose. IBM reported that 60% of cyber-attacks during 2015 were conducted by insiders.[5]

Family offices should ensure they have current signed contracts with each vendor or company they work with. These contracts should describe what the firm is doing to protect the family from human and technology threats, including conducting background checks on their staff at least every three years. Even major institutions such as banks are grappling with cybersecurity obstacles tied to third-party vendors. In our Global State of Information Security® Survey 2017, financial sector respondents reported this as their top information security challenge in 2016.[6]

The family office also should repeat background checks every three years on their own employees, along with household and other staff with access to family houses, offices and resources.

[5] "Reviewing a Year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations," IBM, April 2016

[6] Industry findings: Financial services, PwC Global State of Information Security® Survey 2017

5 *Reinforce good cybersecurity practices with examples and refresher courses*

Family offices can use the best cybersecurity vendors in the country, paired with robust policies and staff, but ultimately it comes down to decisions by each family member or staff. Family members need to understand how a post on social media might lead to a kidnapping[7] or their house being robbed; how logging into their email account at a coffee shop might lead to identity theft and wire transfer fraud; how clicking on an email link might trigger a ransomware attack on the family business' servers; and why using "password" as your home router password could provide hackers easy access to security cameras.

Unfortunately, most of our brains seem to "leak" over time. We need regular refreshers on the threats around us and how to protect the family. One of the most effective ways is to leverage annual family meetings to share lessons learned from actual cybersecurity incidents that have impacted other families and businesses. While this may sound like a scare tactic, the real intent is to create awareness and reinforce the family's policies.

As a possible approach, consider engaging an outside firm to conduct ethical phishing on staff and family members. The results can be used in annual training to ensure family and staff know how to avoid such threats.

What is ... Phishing?

An attack where someone pretends to be a legitimate vendor or employee in order to gather information or to get someone to click on links that expose the network.

It can be done in person, on the phone, via email or even text.

What to do?

Avoid clicking on suspicious links or opening attachments, and abstain from using a work email address for personal business. Phishing emails frequently include misspellings and unconventional formatting.

One in 14 internet users are tricked into following a link or opening an attachment, and 95% of phishing attacks that lead to a breach are followed by software installation.

"2017 Data Breach Investigations Report," Verizon, 4/27/2017

[7] "Southlake father a victim of virtual kidnapping," by Bradley Blackburn, WFAA News, 3/23/2017

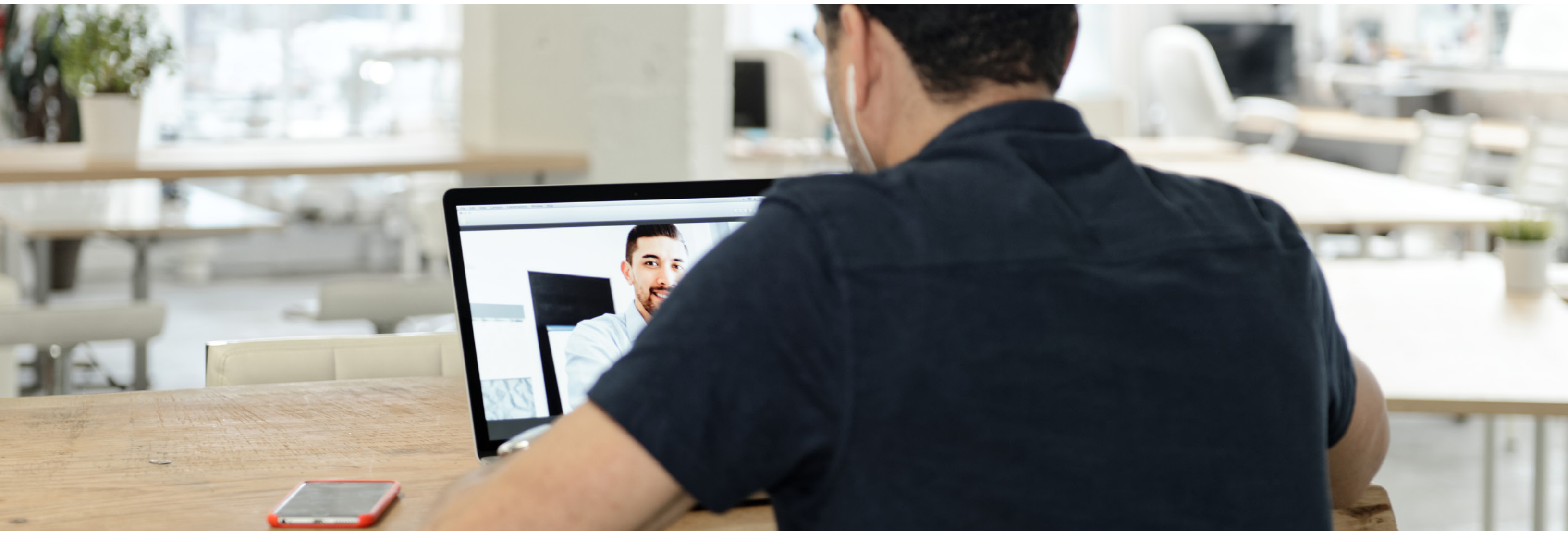
6 *Deploy technology tools and assessments to support protection*

Most of what we've addressed until now covers behavioral and policy challenges. That is intentional, as we believe these areas lead to most of the risk for wealthy families. However, there are several technology areas that should be addressed as well.

- ***Data backups:*** Technical staff should ensure data is backed up. This includes the family office server, smart phones, tablets and laptops. They should maintain multiple backups of each, so clean backups are not overwritten prior to someone discovering there is a virus or ransomware.
- ***Vulnerability assessment:*** Have a technology firm conduct an annual vulnerability assessment, which is basically looking for weaknesses in your technology (equivalent of looking for unlocked doors in a parking lot). These should be done for the family office, for each family member's home and for each business supported by the family office. Penetration testing (pen testing) goes beyond vulnerability by actually attempting to hack or penetrate systems. It is commonly done for businesses, but rarely for family offices (and depending on the family's digital assets, may not be necessary).
- ***Encryption tools:*** Families often need to share tax information with an outside accountant, estate details with their attorney or perhaps business dealings with each other. Standard emails are stored on both originating and destination servers, as well as often sitting on in-transit servers. Any of these devices can be breached. Families can either use secure document storage, where they give a user access to a particular document or folder, or they can use encrypted email tools to secure the emails.
- ***Monitoring:*** Despite the best defenses, highly experienced and determined hackers are often able to breach the systems they target. Family offices should use a technology support partner with monitoring capabilities that can enable real-time responses when hackers strike. In addition, activity logs can be used to detect suspicious activity (including unusual keystroke behavior) and can help in case of a post-intrusion investigation.

7 *Be ready for a crisis: Get the resources and response plans prepared now*

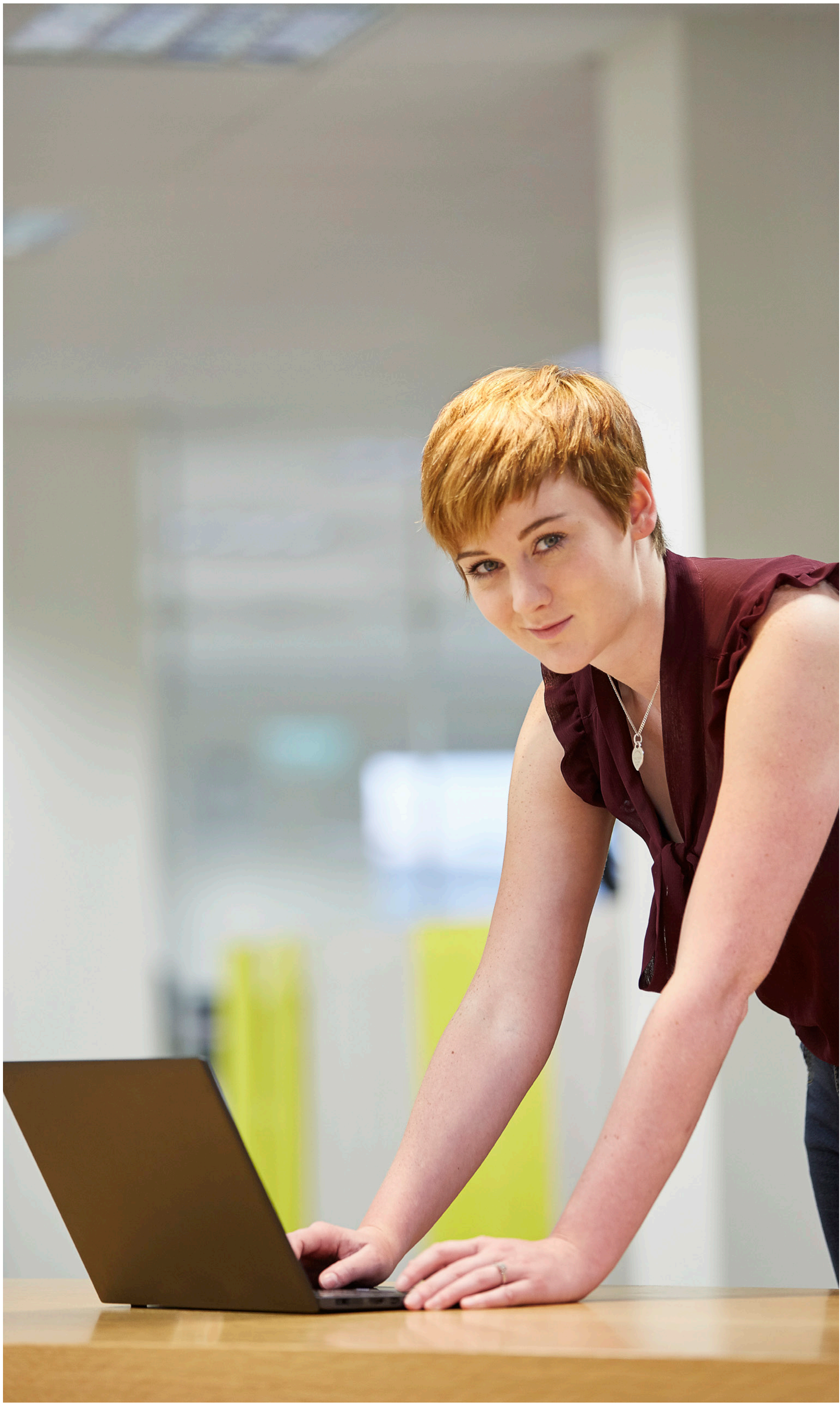
A final component of the strategic cybersecurity plan is identifying how you would respond to a crisis. The plan should address common items such as lost phones or laptops, in addition to which actions family and staff should take if they believe they have a phishing email or phone call. It also should cover how to handle a ransomware event, hacked emails and network intrusions. Consider rehearsing your response to a cyberattack.



Cybersecurity insurance may be an option, but it is still mostly designed for businesses rather than families. They typically cover remediation costs, liability for loss of data and settlement costs, which don't apply to most families. The key benefit for a family may be as a resource to call in the moment of crisis. Cybersecurity insurance, however, is no substitute for proactive risk mitigation.

The worst possible time to think about how to handle a crisis is during the crisis itself. The family office should have a plan for each type of event. Resources can be an outsourced IT support firm, their insurance company or a relationship with a personal security or cybersecurity firm.

As noted recently by Sean Joyce, who was formerly the FBI's deputy director and now leads PwC's US Cybersecurity and Privacy practice, managing cyber risks in a strategic manner requires tradeoffs, just like managing any other kind of business risk.[8] Creating a strategic approach to cybersecurity may sound daunting, but it allows a family to take advantage of the benefits of technology while managing the risks to the family's wealth, security, privacy and reputation.



[8] "Petya just hit...what's next after a global cyber attack?" by Sean Joyce, 6/28/17

www.pwc.com/pcs

More information

Want to learn more about cybersecurity and family offices? Please contact us:

Charlie Carr
US Family Enterprises
Advisory Leader
charles.carr@pwc.com

Jonathan Flack
US Family Business
Services Leader
jonathan.flack@pwc.com

Brittney Saks
US Personal Financial
Services Leader
brittney.b.saks@pwc.com

About PwC's Family Enterprise Advisory Services

PwC's Family Enterprise Advisory Services is part of the Private Company Services (PCS) practice with more than 180 partners and 2,200 staff dedicated to working with family businesses and their owners. Our professionals have a deep understanding of wealthy families, their businesses and their family offices that comes from years of experience working with owners, the family members and their advisors.

We support families through strategic planning, succession planning, setting up family offices, and performing diagnostic reviews of existing family offices to ensure they most effectively support the family and its desired legacy. We help families define what makes their family legacy unique from others and plan for how to sustain that legacy across the family and the enterprise for generations to come.

Visit us online at pwc.com/us/familybusiness