plante moran | Audit. Tax. Consulting.
Wealth Management.

CYBERSECURITY:

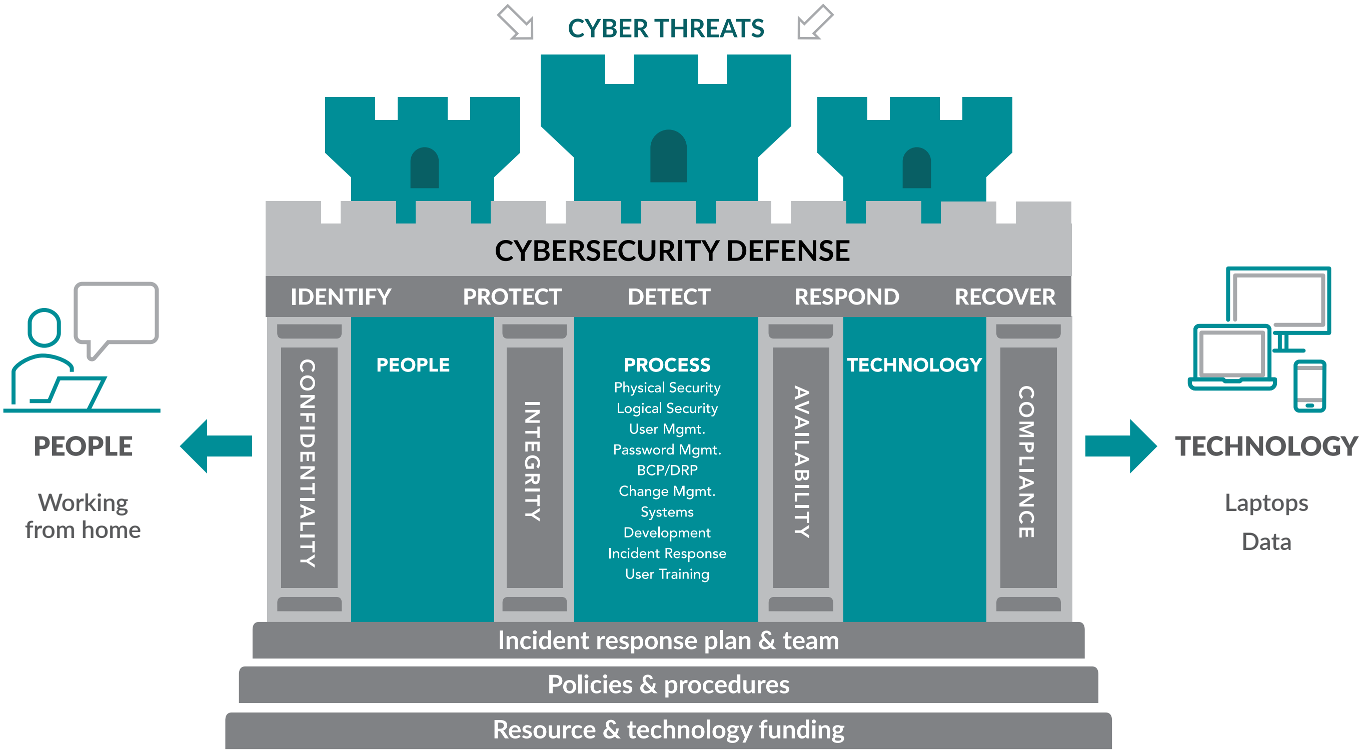
Action items for every family office

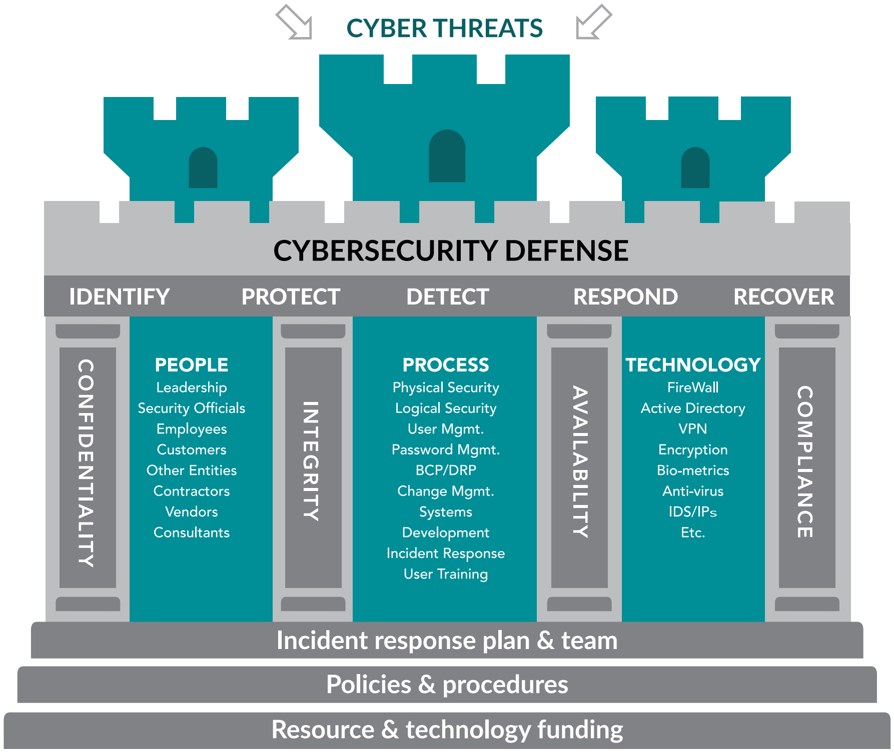
Cyberattacks continue to increase, and family offices are particularly vulnerable to hackers. Family names are well known, and public information is available regarding family wealth, which can put dollar signs in the eyes of cybercriminals. At the same time, family offices are expanding their technology footprint, which requires increased focus on security across a wider range of devices, vendors, and cloud platforms.

The state of cybersecurity at family offices

The threat landscape continues to evolve, but family office defenses may not have kept up with new and developing challenges. Think of your family office environment as a secure castle. Most family offices have many layers of security controls in place. Instead of walls, guards, and moats, layers of controls in family offices include trained **people**, formal **processes**, and strong **technology**, as shown in the image below. Some offices might have a few more archers or sturdier walls than others, but generally, most family offices have put multiple layers in place to protect their internal environment from external threats.

With the start of the COVID-19 pandemic in early 2020, many family offices sent employees to work from home for the first time. Some organizations planned ahead (or got lucky with recent laptop orders) and were able to react quickly to this shift. Others had to rush in new VPN setups and roll out new web-accessible applications. Under normal circumstances, these projects usually take months of effort. Circumstances were anything but normal and, in the interim, many employees worked remotely on their personal devices. Unsurprisingly, best security practices and precautions weren't always followed in the rush to minimize business disruption. In addition, work-from-home options were never really part of the office culture for many family offices, which led to gaps in training, procedures, and controls and required many teams to make important technology decisions on the fly.





As we discussed in "**The new family office 5.0 model**," family offices typically are structured in one of four ways: as single-family offices (SFO), multifamily offices (MFO), virtual-family offices (VFO), and hybrid-family offices (HFO). Each of the four most common family office structures has its own unique security threats. We work with offices across all four operating models throughout the country, with work-from-home trending across the board.

These recent decisions to offer more work-from-home options — regardless of operating model — have brought additional security complications. For projects and remote connections implemented in the last year, vulnerabilities remain. As staff return to the office, with some continuing to work from home, personal devices present a growing risk of bringing viruses to secure internal networks. Meanwhile, attackers continue to increase their profits as they send phishing emails to trick employees into clicking links, often opening up the door for ransomware to spread.

Current cybersecurity threats facing family offices

Based on our work with various family offices each year, we see several common trends in thecritical cyberthreats impacting organizations. Many attacks are successful because family members also have access to office systems. In talking about threats and security, we refer to both family members and employees as “family office system users.”

While unique forms of attack do occur, most family office cybersecurity incidents can be tied back to at least one of these threat areas:

Remote security vulnerabilities

With employees working remotely, the line between secure office networks and home networks blurs, particularly when spouses and children also connect to the same wireless home network with additional devices. The organization may have zero visibilty into the security of any of these devices. This includes being unaware of viruses that may be accessing data on the devices. In addition, many family offices that recently added remote access haven’t added multifactor authentication requirements. This has led to multiple security incidents in which attackers have guessed credentials, gained access to family office system user devices and networks, and were then able to easily view emails and other confidential information.

Lack of dedicated security resources

Many family offices run lean organizations, and smaller office environments tend to result in small internal IT teams or relationships with IT vendors that specialize in supporting smaller organizations. Since IT vendors are often focused on system availability and ease of access, security projects can be seen as lower priority — until after a security breach occurs. Without a strong security teammate or vendor involved in key decisions, IT projects often prioritize efficiency at the cost of security. A key example is staff sharing confidential documents via unencrypted emails rather than using the organization’s secure portal because email seems quicker or more convenient.

Ransomware

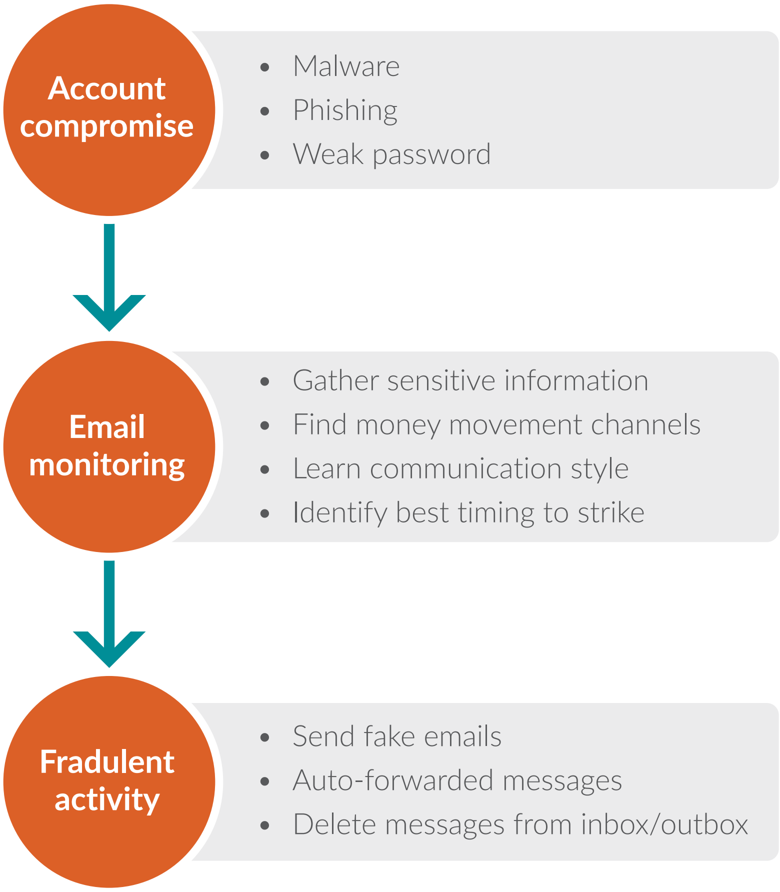
Not only are ransomware attacks increasing, their methods are also adapting as targeted companies find alternatives to paying. Originally the attack would focus on encrypting files and requiring companies to pay to unlock them. Organizations that had reliable backups to restore from could circumvent the hackers. But as more organizations built robust backup controls, attackers have adjusted the threat to focus on publicly releasing data unless ransoms are paid. Attackers are also researching organizations to identify appropriate bitcoin ransom amounts — with wealthy family offices getting hit with higher ransom demands than other companies.

Social engineering

Emails sent to family office system users tricking them into clicking links and providing credentials are still a main channel for attackers to gain initial footholds into family office networks. The COVID-19 pandemic offered many opportunities for attackers to mimic emails with urgent pandemic-related messages. Additionally, employees working at home can't as easily ask an office neighbor if an email appears suspicious. Family members are also at high risk. We often see issues with a family member falling victim to social engineering attacks, compromising their family office email accounts or personal email accounts. Our cybersecurity practice has seen a significant rise in click rates during social engineering tests recently, demonstrating that many end-users still fall prey to fake emails.

Email account takeover

More often than we'd like to hear, family offices reach out after one of the family members has had a personal email account security incident. After attackers gain access, they quietly monitor emails and bide their time before mounting an attack. Having access to years of stored emails can help them pinpoint the ideal timing and approach to, for example, request a change in wire instructions from a family office employee.



Account compromise

- Malware
- Phishing
- Weak password

Email monitoring

- Gather sensitive information
- Find money movement channels
- Learn communication style
- Identify best timing to strike

Fradulent activity

- Send fake emails
- Auto-forwarded messages
- Delete messages from inbox/outbox

Secure your family office against cyberthreats

With so many changes, it’s critical to reassess the family office security environment. Ideally, a family office puts dozens of complex, layered controls in place, but we see common gaps that can lead to security incidents. Focus on these key action items as initial steps to validate your existing security setup and inform your plans to address any shortcomings you identify.

Security awareness training

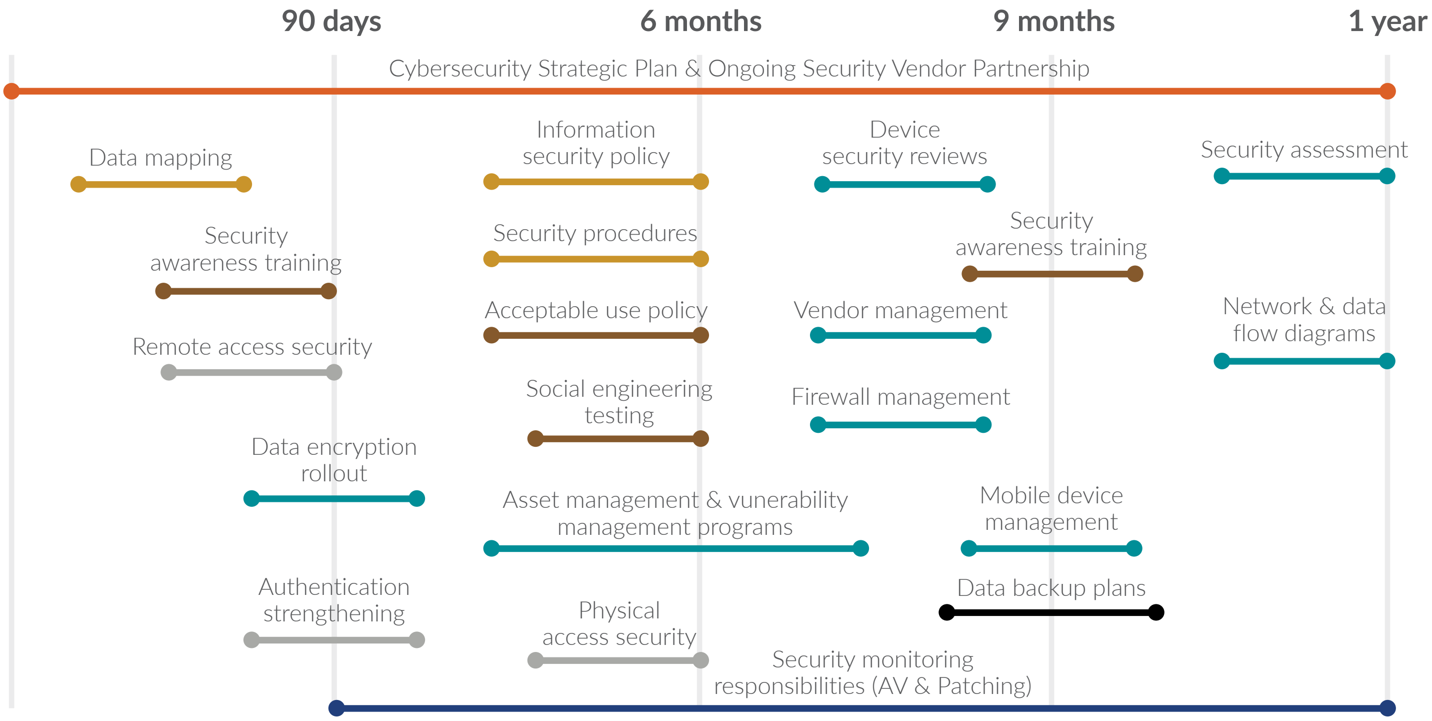
Ultimately, most breaches can be traced back to a family member’s or employee’s quick mistake; for example, opening an email they should have deleted. While technology can protect family offices from many security threats, end-user awareness is a critical control. Security awareness efforts should be ongoing. As IT and cybersecurity threats continue to evolve, family offices should keep both employees and family members updated on trends and best practices to stay ahead of potential attacks.

Multifactor authentication

In a traditional family office environment, teams often benefited from a layered security approach — requiring physical access to an office suite, network credentials, and additional system and application controls all in place to prevent anyone from accessing sensitive data. With many applications becoming accessible online, if all an attacker needs is the right website URL and a guessed password, it’s only a matter of time until you have unexpected visitors in your online accounts. Multifactor options have grown in recent years, ideally allowing your team the ability to offer mobile phone apps, text messages, emails, or tokens as an additional layer to secure login channels. These multifactor options are typically not too burdensome for end-users to use on a daily basis.

Strategic planning

As a bigger-picture item, developing a strategic security plan can — and should — shift the family office away from reacting to issues and toward proactive planning in order to strengthen cybersecurity controls year over year. This effort can help to prioritize projects that address greater office-specific risks, while also ensuring security remains an active, ongoing conversation. All family offices can benefit from a strategic and proactive security plan — whether a heavy overhaul of the security setup is in order or management needs to focus more on updating and evolving existing controls.



Access reviews

Reviewing, in detail, actual access rights in IT systems is usually an eye-opening process for family offices. With typically low turnover among staff, family office executives often comment that access rights aren't a concern. They should be. Employees with widespread access to all systems within a family office are a hacker's winning lottery ticket. The same holds true for former vendors that have administrative accounts still enabled and consultants who only require limited access to support one system but are able to view every file in the office (hope that vendor has great security in place!).

Security testing

Having a second set of eyes to review your controls also can help identify gaps and offer peace of mind regarding existing strengths. Penetration testing can be performed to mimic techniques used by actual hackers. Additional security audits can help identify strengths and opportunities for improvement in areas such as employee training effectiveness, formal procedures, and various implemented security tools.

Bios

While attackers continue to refine their approaches and up their game, implementing these key controls and proactive planning to strengthen your cybersecurity castle walls can help protect your family office.

If you have questions about cybersecurity best practices, please feel free to contact us.

Joe Oleksak | Partner
847-628-8860 | joe.oleksak@plantemoran.com

Joe is a cybersecurity partner and leader of the firm's family office cybersecurity team. He provides family offices with a variety of security assessment services, including security consulting, penetration testing, and ongoing cyber advisory assistance. Joe also frequently presents to family office boards on evolving security threats.

Colin Taggart | Principal
248-223-3235 | colin.taggart@plantemoran.com

Colin is a cybersecurity principal and leader of the firm's family office cybersecurity team. He leads security assessments for family offices, including ongoing cyber advisory assistance for multiple organizations. He frequently consults with family offices responding to recent security breaches.