



Helena Robertsson, EY

Helena Robertsson leads EY's Global Family Enterprise platform, comprising a network of trusted advisers who facilitate the success and growth of family enterprises by helping them design long-term strategies and implement the right tools, skills and training to succeed. Her core specialty is tax advisory with more than 20 years' experience helping clients in Nordic countries and internationally.

Cybersecurity risks family enterprises and offices face during COVID-19

Helena Robertsson

Cyberattacks are accelerating as criminals and other threat actors seek to exploit the disruption caused by the coronavirus (COVID-19) pandemic. Businesses have scrambled to implement sweeping remote work practices and online-only interactions with employees, customers and vendors. These changes have come with heightened cybersecurity risks. Some family enterprises and family offices are recognising the danger, and taking steps to increase cybersecurity capabilities, however, others need to catch up quickly.

Even before the pandemic, some family enterprises and family offices were lagging in cybersecurity practices. Historically, cybersecurity in family offices and smaller family enterprises has focused on finances (for instance, making sure money is not transferred mistakenly or fraudulently). But as information has moved to the cloud and social media, the walls of these businesses have expanded—opening many more opportunities for attacks.

Threats from all directions: phishing, data theft, remote work

According to a recent article by EY global advisory cybersecurity leader Kris Lovejoy, the rush to remote work and the general sense of

panic set off by COVID-19 has opened the door to a wide range of additional cybersecurity risks that family enterprises must attend to urgently, outlined as follows:

- **Increased remote work**—threat actors are taking advantage of cybersecurity holes caused by widespread telecommuting (e.g. increased pressure on IT teams, users bypassing cybersecurity leading practices, and remote administration of critical information).
- **Increased phishing and malicious content**—threat actors have significantly increased their use of phishing, malicious sites and business email compromise attempts linked to the pandemic.
- **Increased data theft**—threat actors conducting data theft for extortion, disruptive or destructive ransomware attacks, and/or seeking to damage enterprises' brands have targeted organisations perceived as being under pandemic-related strain.

"COVID-19 has made it more pressing than ever that family firms develop control structures that create a protective stance and readiness to respond." (Paul McKibbin, EY Americas family office advisory managing director)

The principal risk

family offices and family enterprises add yet another risk to this list, that is, the families themselves. In family offices and smaller family enterprises, the person in charge of IT may not have control over the

actions of principals and their family members. There may be no chief information security officer with a tight rein over devices, access and usage, as there is in large enterprises. Instead, there may be a small group of staff that must try to manage IT controls with governance, frequent education and personal influence.

Family members range from tech-savvy teenagers to tech-averse octogenarians and everyone in between. They may use personal emails or follow substandard mobile security practices, leaving them—and their family firms—open to malware, phishing attacks and wire fraud, all on the rise during the pandemic.

Example. Opening the door for cybercriminals

If a principal is dedicated to using a non-supported android phone and routinely downloads non-supported apps from unapproved app stores, they are very likely to accidentally install malware, handing full access over to an attacker.

That attacker may spend months monitoring the victim's correspondence, their movements and their communication style to mimic them effectively. They can then use this knowledge and access to issue disastrous directions to employees, like ordering an employee to make a seven-figure wire transfer using the principal's own mobile device and email account.

In the COVID-19 environment, loose cybersecurity practices mark family offices, smaller family enterprises and principals as easy targets for attack.

"Much of the reputational risk is in their broader footprint, out in the world, not within a server. That information footprint is less in their control." (Haris Shawl, cybersecurity senior manager, Ernst & Young LLP)

Reputation and privacy must be protected

At their most severe, cyberattacks can be devastating to a family firm's legacy. An attack could threaten reputation by associating the family's name and brand with a scam or unreliable product, or it could bring down systems, leading to a serious disruption in customer service or employees' ability to work. In research completed for the latest EY Global Capital Confidence Barometer, 24% of 394 family enterprise leaders in middle-market companies named reputational damage as their greatest fear related to cybersecurity.

"Cyber threats are increasingly placing family firms' reputations at risk in a way that many are not yet sufficiently protected against." (Adam Wright, cybersecurity managing director, Ernst & Young LLP)

For many family enterprises, the brand is synonymous with the family name, and that name carries tremen-

dous social capital. When the family name is tarnished, so is the brand. For instance, one very well-known family name was used without the family's consent to sell dubious financial products via social media. The family had spent years carefully curating their name and their brand, ensuring that it is associated only with the products, services and causes they believe in. Now the brand is at risk through no fault of their own.

Family offices also carry data privacy risks, and when private family information and correspondence are stolen or leaked, it can create serious reputational damage and risk of litigation. With only a handful of employees, family offices have limited tools and talent to monitor and ensure the data privacy of the principals. Even when they invest in leading-class cybersecurity technology, too often they take a 'set and forget' approach. Further, the systems are doing what they are supposed to do, but family offices lack the in-house expertise to monitor and act on what the systems are telling them.

A family office sometimes sits within the family enterprise so it can leverage the resources of the larger organisation. However, that model puts private family information in the same systems as family enterprise business information, where it is subject to additional threats from inside and outside the family enterprise.

Cybersecurity steps for family enterprises and family offices in the short and long term

The good news is that there are steps family enterprises and family offices can take to protect their firms and families in order to lower these risks.

"Those organisations that really push for that proactive involvement of cybersecurity are going to see very significant business benefits in both the near term and the long term," says Dave Burg, EY Americas cybersecurity leader. This will require both immediate steps and a long-term change of approach.

In the short term, to fend off the increase of cyberattacks due to the pandemic, family enterprises and family offices should:

- make and keep an inventory of all routers and devices, and sensitive data on them, including those used in family members' homes
- maintain these devices with updated antivirus and firewall software, and keep all software current and assess for vulnerability at least annually
- use email encryption tools for any confidential messages and ask clients to validate any new account openings, credit requests and similar activity
- monitor (or use an external firm to monitor) all networks 24 hours a day, looking for signs of an intrusion and shut them down if there is an attack
- store backups offsite or in a secure cloud repository
- conduct financial and criminal background checks on new staff and vendors, and annually thereafter
- create a cybersecurity policy that includes connected



The quote

In the COVID-19 environment, loose cybersecurity practices mark family offices, smaller family enterprises and principals as easy targets for attack.

devices, passwords, multifactor authentication, social media and payment authorisation steps.

In the longer term, family enterprises and family offices need to:

- change the way they look at cybersecurity
- recognise that breaches and social media threats will happen
- understand that the job of the family enterprise and family office is to respond effectively and minimise the damage.

Further, family enterprises and family offices must work closely with principals, their families, and employees to:

1. identify the scenarios that would impact them most, their risk tolerances and their pain points
2. analyse the most likely scenarios and rate the risk level for each
3. customise a robust controls framework (e.g. the National Institute of Standards and Technology (NIST) Cybersecurity Framework) for the organisation to measure and mitigate risk to an acceptable level
4. explore, create and—most importantly—test business continuity and incident response plans regularly
5. continually educate all principals, family members and their households on the importance of adhering to these controls and the risks they face if they do not.

Protecting the legacy

Family firms need to protect their names, their brands and the organisations they have built over generations. Failure to do so can be catastrophic, but the right approach, security technologies and control structures can help them protect their legacies for years to come.

Summary

Cyberattacks and cyber fraud are rising rapidly during the COVID-19 pandemic. These can be devastating to a family enterprise's reputation and legacy. Some family firms are taking steps to increase cybersecurity capabilities, but others are lagging. Family enterprises can protect their legacy if they act quickly and decisively. **FS**