PKF
Funds and Family Office
New York | London | Dublin | Jersey

Funds and Family Office COVID-19 Accelerator series

Our COVID-19 Accelerator series highlights the impact the coronavirus pandemic is having on wealthy families, their offices and businesses. We focus on areas where COVID-19 will accelerate change.

In our second article, we look at the way COVID-19 is accelerating technology adoption and utilisation for wealthy families and the data and cyber-security risks you should be aware of during the crisis and going forward.

This has been a time of upheaval – and learning

In the three months since COVID-19 was declared a pandemic, our world has been twisted upside down and inside out. While our physical contact with other people has been restricted, the digital world has exploded.

Zoom's subscriber numbers have increased dramatically, we have become masters of the virtual meeting and the consumption of digital content has gone through the roof.

Lockdown has forced everyone to review their business continuity planning, protocols, processes and governance so that they can maintain and support their human, intellectual and financial capital.

As business capacity has been stretched and IT infrastructure tested, existing processes have been pushed to breaking point and are now being renewed and refined.

While families, their businesses and offices become increasingly reliant on their digital capability, it is essential to consider some of the key learnings of this extraordinary time.

How will your business need to change?

The future operating model of your business and your office is likely to be a hybrid that embraces remote working. Automation tools such as robotics process automation (RPA) and workflow collaboration applications can reduce the time spent on manual tasks. That lowers the risk of human error and keeps data more accurate, up to date and secure.

RPA can be applied to areas such as gathering documents and data for processing, document management, tax returns and integrated reporting.

Data security is a key consideration. Campden's Global Family Office report for 2019 found that 20% of family offices suffered a cyber-attack last year.

That threat has risen during lockdown. A Check Point Software & Dimensional Research survey found that 71% of IT and security professionals have seen an increase in security threats since the pandemic began. Just over half (55%) cited phishing attempts as the main threat, followed by malicious websites offering advice about COVID-19 (32%) and increases in malware (28%) and ransomware (19%).

Make your communication clear and consistent

In a time of crisis, getting your communication right is critical. Even on a Zoom call, it's not easy to pick up on body language and other non-verbal communication. To keep your family enterprise aligned, it's essential that your communications are consistent, authentic and personal.

As well as your daily and weekly crisis updates and management meetings, be sure you find time for family social connections and regular updates for the people in your family enterprise. It's a good way of reminding yourselves why you choose to stay together.

Upgrade your risk management

There has never been a greater need for a robust cyber-security strategy. Your personal security is at risk from webcam extortion, identity theft and new threats related to working and studying at home. Your office security could be vulnerable to authentication weaknesses, email account takeovers and the risk that vendors could be compromised.

Recent social engineering and ransomware developments represent an extra level of risk to any business, employee or office.

Your cyber-security strategy should take into account the risks that can be created by employees, suppliers and vendors, accidentally or on purpose.

Make sure you have a current, signed contract with every vendor, supplier or company your family office works with. This should describe what they are doing to protect the family from human and technological threats, including background checks on staff at least every three years.

Similarly, your office should carry out background checks just as often on your employees and other staff with access to family houses, offices and resources.

Data security guidelines

- Know what information you have, where it is located, how it is protected and who has access. Use a personal information assets register.
- Use encrypted devices. If they are lost or stolen, your data is protected.
- Stop emailing unprotected documents. Use passwords on files.
- Set up secure storage locations for sharing files with auditors.
- Be aware of the following threats:
    - Phishing and whaling are on the increase – be careful what you share. Develop a complete picture of your personal profiles.
    - Ransomware, which encrypts your files and demands a fee for unlocking them.
    - Traditional fraud, which plays on heightened fears during the pandemic.
- Be careful what you share online.
- Keep your devices updated. Be aware of security patches, which are being released at an increasing pace.
- Test your home network for vulnerabilities (see below).

Cyber-security guidelines

Be aware of the threats listed above, and of agencies with good advice to help you such as Action Fraud, Cyber Aware and the National Cyber Security Centre.

You should also take the following steps:

- Obtain external accreditation for your family office digital environment and your information management policies.
- Review, update and test your back-up capability and disaster recovery protocols regularly.
- Train your teams in cyber-security, especially in information asset management.
- Constant monitoring. Knowing how many phishing attempts are made ensures high awareness of the threat.
- Update and test your cyber-security incident response plan.
- Manage your user privileges and ensure everybody gets only the access they need.
- Undertake home vulnerability scanning to identify issues with your devices, network and internet connections.

Prepare for the next crisis now

With the actions you have taken in response to COVID-19 fresh in your mind, this is the ideal moment to review those actions and apply the lessons learned to a new, updated data and cyber-security plan.

Central to this plan will be the measures you will take in a crisis. These will include actions when phones or laptops are lost, and when you suspect you have received a phishing email or phone call.

Your plan should also cover your response to a ransomware event, hacked emails and network breaches. You should use your new plan to rehearse your response to a cyber-attack.

A family enterprise should have a plan for each type of event, either monitored in-house or by an IT support firm, insurance company or trusted business partner.

What next?

If you, your family or your client family would like to know more about how to respond to any of the issues raised in this article, contact us for further information or advice.

Contact us

Paul Pratt, Commercial Director
D: +44 (0)20 7516 2233 | M: +44 (0)7825 257457
E: ppratt@pkffundsfamily.com

PKF Littlejohn LLP, 15 Westferry Circus, Canary Wharf, London E14 4HD
Tel: +44 (0)20 7516 2200

www.pkffundsfamily.com