Cyber and Financial Advisors

DO YOU…

1. Make electronic payments with either client money or your own?
2. Work remotely, or from multiple locations, and do you require wet ink signatures on contracts?
3. Rely on a cloud provider or third-party IT business to store and manage your data?
4. See your brand and reputation as key to your continued success?
5. Know who you would contact in the event of a cyber attack or data breach?

Exposure and Risk Management

1. Electronic payments raise a raft of exposures but the most common is falling victim to an invoice hijacking or social engineering scam. To ensure damage to your finances is kept to a minimum, we recommend using 2 factor authentication for all new or amended payees

2. The dangers of working remotely are twofold. Firstly, public networks are unsecure so where possible, avoid connecting to them for work purposes. Secondly, loss of work devices containing client information is a personal data breach under GDPR. This could be leaving a laptop at the golf club, leaving a USB stick on a train or even as simple as leaving a signed, paper contract in a restaurant. Remembering, of course, that Cyber insurance covers losses for physical data as well as electronic data. To reduce this exposure, we suggest password protecting or encrypting all mobile devices and connecting via a VPN if using a public network is unavoidable.

3. Outsourcing your IT is a fantastic, cost effective way of managing your data but remember that Cloud Providers are a business like any other and can be hacked or exploited in the same ways. If your cloud or managed service provider loses your data, you will remain responsible. You may be able to claim compensation by entering extensive legal proceedings, but you will have no support to ensure your survival in short term. To find yourself with no network, no contacts, no files and no way of reaching your clients would be disastrous. It is good practice to include a section on cyber attacks and data breaches within your business continuity plan and ensure all critical data is backed up at least every 7 days. It may be easy to pick up where you left off following a fire, but a ransomware attack that completely wipes your files or database may not be so easy to bounce back from.

4. As a financial advisor, we understand that your reputation is everything. Without a sound reputation, referrals do not exist, and trust cannot be gained. It would be a shame, therefore, to see it tarnished due to a cyber attack, human error or data breach. Your clients trust you implicitly and losing their data, money or trust will have an adverse effect on your profits. Although a loss of profits attributed to a cyber event is covered by a cyber insurance policy, it is best practice to ensure your governance and policies on data protection and privacy are substantial and kept up to date.

5. Most businesses are more than aware of who to contact in the event of a fire, flood or theft but who would you contact in the event of a cyber attack, human error data breach? If the answer is “I’m not sure” or “our IT people”, we suggest revisiting your continuity plans and engaging the services of proper, cyber incident responders. Cyber incident response teams can be contracted in, as and when required, or engaged and paid for by an insurer if you have a live cyber insurance policy.

How will an Optimum Cyber Plus policy help?

1. Up to £100,000 of E-theft cover can be included within our policy. Cover extends to include social engineering losses and does not require there to be a breach of your network to respond. All policyholders will also receive a suite of online training modules on cyber crime and data protection to ensure your staff are doing all they can to keep you protected.

2. Our policy will engage for loss of data in all formats. It is for this reason that paper files and contracts are covered in the exact same way that electronic files would be. In addition to this, employees of all policy holders will receive online training modules on the do's and don'ts of working remotely.

3. Our policy extends to cover losses resulting from any unplanned system outage, network interruption or degradation of a Cloud Service Provider's network, as well as your own.

4. Cover is granted for damage to your reputation via adverse media, including social media, caused solely by a cyber or data liability event.

5. All policyholders have access to a team of cyber incident responders 24 hours a day, 365 days a year. In the event that you suffer an attack or breach, our incident responders will make contact and begin working to resolve the situation within 120 minutes of notification. We do not charge an excess for this service as we want you to lean on us as emergency responders for every event.