Can you put your trust in cyber space?

It seems that almost every week we read of another cyber breach at a well-known organisation. High profile celebrities recently had their privacy compromised with the leak of personal photos from the cloud, millions of small business records were compromised at a large financial institution and tens of millions of customer account details have been stolen from retailers. So what steps can be taken to strengthen individual and family office cyber security?

In today's digital world, we all have a bigger online footprint than we might realise. We routinely communicate, interact and store information online and increasingly do so across public networks via mobile devices, from phones to tablets.

Connected lives and businesses

Frequent travel may take individuals to 'high risk' countries where information security could be compromised. Home and family office systems could be targeted, or staff could be the subject of phishing attacks where an outsider impersonates a supplier or bank. When making investments or completing financial deals, how do you know you are transacting with your financial institution? Home systems, which may also interface with family office systems, could be a weak link. Social contacts – family, friends, other business colleagues or public figures – who may interact digitally through social media such as Face book, Twitter, LinkedIn and Instagram, can result in a rich picture of an individual's life that is extremely valuable to those planning a targeted attack.

Faced with such a seemingly endless set of risks, it may seem difficult to know where to start. But with the right approach, it's possible to take more control of cyber risk and move forward on the front foot.

Who are the cyber attackers?

Cyber attackers usually fall into one of several categories. Many of them are organised criminals who are quite simply looking to make money by stealing information and selling it on. They will look for any target where they can see the possibility of financial gain. Then there are 'hacktivists' who are usually motivated by political considerations or some kind of cause. So an individual active around any kind of emotive or contentious issue, could become a target. And the higher the profile of an individual (for example, appearing in a 'rich list' or similar) then the more likely that individual is to be singled out.

Another common threat – sadly – is that posed by insiders. A large proportion of fraud and financial theft is very often carried out by those inside organisations who are trusted by their employers and have access to systems and information.

Where do I start?

Firstly, identify the risks to assets – so as to gain a clear understanding of what is important for the safe running of the home and family office and the security threats faced that might steal or disrupt the things that matter.

Then assess the potential impact of those risks and the degree of exposure to them.

Having done this, remediate those risks. There is much that can be done. This could range from a new approach to travelling by taking a "clean" tablet and phone when travelling to high risk countries, to removing personal data from a digital profile, to ensuring that certain fundamental

security controls such as firewalls, anti-virus software, secure configurations and security logging and monitoring are all in place on laptops and systems.

Finally, because the cyber threat is an ever-evolving one, continuously **monitor** the effectiveness of home and family office systems.

A positive approach

By taking a positive and proactive approach to managing cyber risk, individuals and family offices can get ahead of the risks and put themselves on a stronger footing to flourish.

Questions to consider [format as call-out box]

- Do you have the right level of protection for the data and systems that are critical to your home and family office?
- What would the impact be on you or your home and family office if you suffered a cyber security breach?

"We believe cyber security should be about what you can do – not what you can't"

Author's details:

Matthew Martindale

Director, Cyber Security, KPMG

T:+44 (0) 79 1755 2588

E:matthew.martindale@kpmg.co.uk

Visit our website to find out more www.kpmg.com/uk/cyber