Cyber Security & Digital Privacy

What Family Offices Need to Know

MARCLAY ASSOCIATES

Executive Summary

Protecting servers and filtering malicious emails rarely stay on the agenda for long in a small business or family office. But in the face of increasingly complex cyber-attacks, high-value families, celebrities and other high-net worth individuals are under growing pressure to pay closer attention to their security and digital privacy.

Cyber-attacks are becoming ever more sophisticated, as well as more frequent. Cloud computing, the proliferation of 'big data' and the growing use of mobile devices, tablets and social media are creating new and significant security challenges.

The impact can be far-reaching. Recent high profile incidents show that cyber-attacks can not only strike into a company's finances, but also inflict unquantifiable reputational damage.

No-one is immune.

Who's at risk?

Cyber crime is one of the top threats facing individuals and small businesses, according to the World Economic Forum's 2013 Risk Report.

It is no surprise that the UK government rated cyber crime a Tier 1 threat in its 2010 National Security Strategy, and has set aside £650 million to tackle it.

The private sector, too, is waking up to the cyber threat. It is a sign of the times that nearly half the 293 graduates recruited by BAE in 2013 will join its cyber and security division.

Family offices are becoming a high-value target for cyber criminals.

Cyber attack?
It will never happen to me!

Despite the enormous cost to family offices, breaches of cyber security are rarely publicly reported.

Jake Hockley, partner at Marclay Associates describes a recent example of cyber espionage using the latest techniques:

> *"Imagine the scenario: Richard and Keith are competitors in business. They frequently bid for the same contracts which Keith wins around 80% of the time. Richard is angry, he has tried all legitimate ways to compete with Keith but has so far failed.*
>
> *Richard hatches a plan. He decides that the only way to move forward is to fight dirty. This means access to the private information that Keith uses to make his business decisions. Richard has an idea: Get access to Keith's personal and work emails. He knows that this will yield valuable professional and personal details which can be used to outbid Keith or at least damage his reputation. He also knows that Keith relies heavily on his mobile phone and laptop to stay connected as he travels on business.*
>
> *Richard calls a private investigator (PI) that he employed before. The PI agrees to take on the job and buys a device from the internet for $150. The device will discreetly trick Keith into revealing his email account details.*
>
> *The PI searches for Keith on Google and finds that he has an extensive online presence. By checking comments on Facebook, LinkedIn and Twitter the investigator is able to establish that Keith is due to speak at a drinks reception followed by a conference in a central Munich hotel on Tuesday and Wednesday. Bingo! The PI, using an assumed name, books a room at the hotel on the Tuesday night.*
>
> *On Tuesday the PI checks into the hotel and sets about his task. He gets his laptop and device out and connects to the hotel internet. His device is a clever bit of kit. What it does is broadcast a free Wi-Fi signal, using any name the investigator gives it, for people to connect to. The investigator calls it 'free hotel Wi-Fi' and lets it run. But this device has a trick. Anybody that connects to it will be able to*

Who's responsible?

Cyber criminals come in all shapes and sizes*:

- Competitors or foreign intelligence services interested in gaining an economic advantage for their own business or country;
- Hackers who find interfering with computer systems an enjoyable challenge;
- Hacktivists who attacking for political or ideological motives;*
- Employees or others who abuse their legitimate access, either a by accident or deliberately.

*According to the UK Governments Business Guidance 2012

access the internet as usual, but will be blissfully unaware that all the information they access will be visible to the investigator. He can even download all the data to a USB drive to view and analyze later. The investigator settles in. The trap is already laid, all he has to do is wait.

At 9pm, a tired Keith returns to his hotel room. Keen to check up on his work email quickly before going to bed. He opens his laptop and tries to connect to the normal hotel Wi-Fi, which we know is not working. This fails and he sees 'free hotel Wi-Fi' in his available networks bar. He connects and goes straight to his work email login page and enters his email address and password. He gets access to his account and starts to check his email.

Upstairs, in the comfort of his hotel room, the PI checks his computer and realizes that he has got what he came for. He also has logon details for several other delegates who fell for the same trap. Perhaps he may use these as extra bargaining chips. But now he shuts down his computer and goes to sleep, job done. In the morning he checks out and is never seen again.

His report goes to Richard, who now has the email address and password for Keith. He does not intend to change the password of the account, not yet at least, but can now access all the inbox, drafts, outbox and will be able to read future messages. This has given him a commercial advantage, but he also learns that Keith has a complicated family life. Out of interest he checks the same passwords for Keith's Facebook and Twitter accounts. He now has control of those too.

Soon, Richard increases his market share. Keith cannot understand it but it now seems as though Richard is able to compete as never before. Unknown to Keith every discussion he has regarding pricing is closely monitored by Richard, who is then able to undercut by a small percentage every time.

Two weeks later Keith loses access to all his accounts. His colleagues tell him that they have been receiving strange emails from him, radically changing business strategy and behaving aggressively. He finds that he has to phone all his business contacts to explain that it was not him who sent the emails. Some are ok with this, others take a dim view of Keith's apparent lack of security. Trust has been broken."

"…unaware that all the information will be visible to the investigator…"

"…two weeks later Keith loses all access to his accounts…"

Do you have cyber security principles in your office?

Figures produced by a US intelligence agency highlight that 80% of cyber-attacks could be prevented by adhering to basic principles. Security advisors can put a lock on the company's virtual front door by making sure that employees remain fully aware of the risks faced to their office.

A simple policy covering the secure use of the organisation's information – such as restricting the use of portable media and content downloadable from the internet – should be put in place, supported by staff training on digital do's and don'ts.

A further solution is to invite a cyber security firm to test your systems and products for security vulnerabilities.

Those closely involved with a company, but beyond its walls, should not be overlooked. Non-executive directors, for example, work primarily off-site with high level and often confidential information stored on a range of mobile devices which, unlike those used by employees, are typically not protected.

Supply chain and professional service providers can also put sensitive information at risk. In October 2012, NASDAQ halted trading in Google shares when Google's financial printers prematurely released their earnings report. The leak, combined with the weak results it contained, wiped $22 billion off Google's market value.

What's the cost?

A 2011 UK Cabinet Office report estimates that cybercrime costs the UK £27 billion annually:

- £2.2 billion of this to government
- £3.1 billion to individuals via fraud and ID theft
- £21 billion to businesses, in the form of theft of confidential data

Reputational damage, however, can be the biggest cost: it is impossible to quantify the long-term damage to a business's public perception following a cyber-attack.

Research shows that consumer trust, once lost, is very difficult to regain.

Working with your security advisor

Security experts can help you understand and prioritise the cyber risks facing your office and agree its most appropriate line of defence.

Regular dialogue between you and your technical security advisor is essential, but should inform family board discussion, rather than being seen as an end in itself.

Duncan Hine, a Fellow at the Cyber Security Institute at Warwick University recently commented: “Inviting a cyber-security advisor to present at board meetings will help directors better understand cyber threats to the business and the actors behind them, but it’s not the answer to getting a handle on cyber risk management and really controlling the risk.”

By having regular conversations on how the company’s cyber security strategy links into the overall business strategy, chairs will find it easier to translate IT risks into business risks and to communicate these risks to the wider business.

A further consideration is contingency planning. Once a breach has been discovered, early response is often critical to preventing further damage. It is the board’s job to work with the security advisor to ensure the office as a whole is ready for the operational and reputational impact of a successful attack.

Ask the right questions

- Can I be confident that my most important information is being properly managed, and is safe from cyber threats?
- Are we clear that family members and the board are likely to be key targets?
- Do we receive regular intelligence from our security advisor on who may be targeting our company, their methods and their motivations?
- Are we confident that we have identified our key information assets and thoroughly assessed their vulnerability to attack?

Conclusions

In the past, if you asked a family office or board member what kept them awake at night, few would have mentioned the challenge of securing intellectual property assets or managing the risk of sensitive private information being compromised.

In today's environment, however, where 90% of the world's data has been created in the last two years alone, cyber crime presents a serious threat.

Faced with intensifying and highly sophisticated cyber attacks, we are under mounting pressure to treat cyber security as a key business and personal risk.

If you are advising family offices, you have a crucial role to play in considering the types of attacks they may be facing, and the financial, operational and reputational implications of a security breach.

Advisors are also responsible for making sure their offices adopt an integrated, business led approach to cyber security, working closely with advisory firms to ensure that your office security infrastructure is robust and fit-for-purpose.

Cyber security must have the attention everyone advising family offices.

Further Advice

- **10 steps to cyber security**: advice sheets, 2013 - Click Here

- **The UK Cyber Security Strategy**: Protecting and promoting the UK in a digital world - Click Here

Useful Websites

- **Cyber Incident Response** - a scheme launched by GCHQ which helps companies in dealing with a cyber attack - Click Here

- **Action Fraud** - the UK's national 24/7 fraud and cyber crime reporting centre - Click Here

MARCLAY ASSOCIATES

About the author

James Tamblin is a security advisor who specialises in cyber security and investigations. He began his career in covert military intelligence and has recent private sector experience advising family offices, banks, and telecommunications and FMCG businesses across Europe, the Middle East and the Americas.

James holds a BSc (Hons) in Computation from UMIST and a diploma in Intelligence Management.

Regency House
61a Walton Street
Walton on the Hill
Surrey
KT20 7RZ
United Kingdom

W: www.marclay.co.uk
E: info@marclay.co.uk
T: 0845 875 0702

© Marclay Associates 2013