



Cyber threats to family offices

How a resilient approach in the family office can thwart today's cyber threats

From sensitive data and investments to connected devices, cyber threats can impact on many aspects of the family you are charged with protecting. Understanding cyber attackers and their tactics is key to defending the family and the family office. In this report, we have shown that a ten-step approach to cyber security can help family offices withstand a wide range of cyber attacks.

Executive summary

Cyber threats to family offices are numerous and real¹. Extortions, frauds and cyber-enabled physical threats can have a significant impact on the family offices' finances and reputation, and on the safety of the family themselves.

The latest report by Campden research highlights how in 2017, 32% of family offices suffered losses from cyber attacks, in one case costing over \$10 million². Despite this, 48% of respondents did not have a cyber security plan in place.

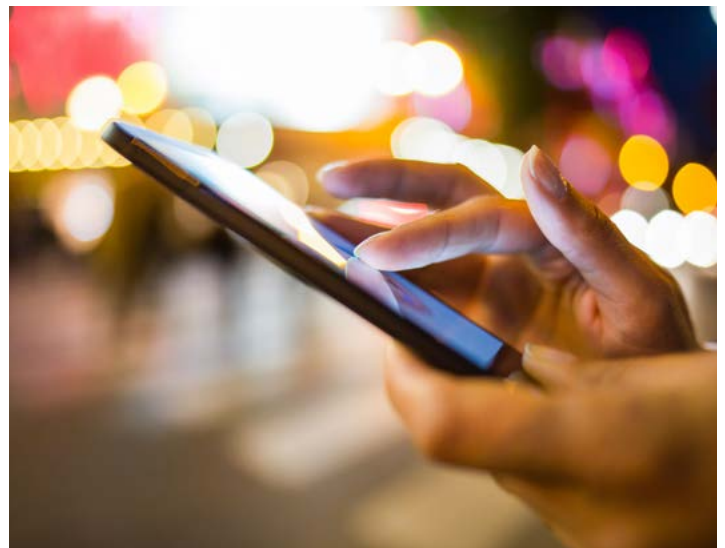
Cybercriminals usually target entities dealing with large sums that are perceived as having insufficient cyber security maturity. As such, family offices represent attractive targets for cyber attackers.

Furthermore, family offices are in possession of sensitive data similar to that of larger organisations. However, their security controls requirements are much less stringent than most large organisations. This is partially because they typically rely on a small number of staff which means that data is often less segregated and more exposed than it is in larger organisations³. However, basic security precautions can have a disproportionate effect in preventing cyber attacks. For example, simply implementing strict password policies, and keeping your anti-virus software up to date can have a huge beneficial impact.

In this report, Deloitte has identified ten key actions that family offices should consider implementing to prevent, detect and respond to cyber incidents. The second part of this report will focus on the top ten strategic controls which are inter-dependent and when combined provide a foundational cyber defense to effectively minimise the family office's exposure to cyber threats.

We also touch upon threats to the family members themselves. For instance, family offices should consider how the increased use of connected devices, including phones, tablets, cars and smart speakers increases the exposure to cyber intrusion of the family members they represent, their vehicles and homes. An assessment of each threat, including real-life examples, is discussed in the first part of this report.

Although family offices increasingly offer a range of services outside of the financial space, cyber security still remains mostly outsourced. This report will therefore provide you with a good understanding of the threats you face and enable you to ask the right questions to your cyber security provider.















1. citywire.co.uk/wealth-manager/news/why-family-offices-need-to-up-their-game-on-cyber-security/a1071874

2. ubs.com/global/en/wealth-management/uhnw/global-family-office/global-family-office-report-2018.html

3. europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Threats overview

The table below highlights the most likely threats that family offices and the families they represent may face at work, at home, and in transit. The table shows where each threat is most likely to manifest based on the most common attack vectors used by threat actors and the systems they target. A more detailed assessment of each threat, including real-life examples, is discussed in the next section of this report.

Threats	At Work	At Home	In Transit
 Extortion <ul style="list-style-type: none"> Ransomware Blackmail to publish sensitive data 			
 Fraud <ul style="list-style-type: none"> Business email hack Social media account hijacking 			
 Espionage			
 Cyber-enabled physical threats <ul style="list-style-type: none"> Information gathering and unwanted attention Vehicle compromise e.g. superyachts and cars High value homes and estates compromise 			



Extortion



Ransomware

Ransomware is a type of malicious software (malware) that gains access to your computer or office network and scrambles your files in a way that only the attackers know how to reverse. Ransomware is widely exploited by cybercriminals against both individuals and organisations, and costed the global economy an estimated \$5 billion in 2017⁴.

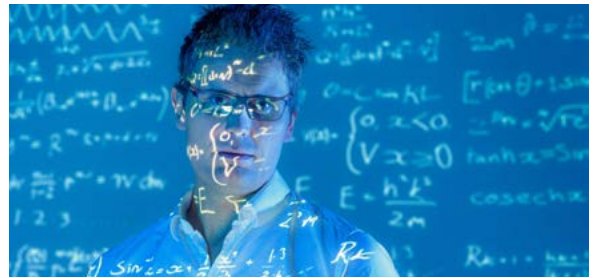


Case study – Dridex delivers bespoke ransomware to targets

In September 2018, the cybercriminal group behind the Dridex malware began conducting targeted ransomware attacks. The group conducts assessments of their victims to determine security measures in place and customise the attack to avoid the specific antivirus used. The group carried out at least 200 successful attacks, demanding ransom amounts of between £15,000 and £300,000 from each victim⁵.

Blackmail to publish sensitive data

Cybercriminals infiltrate an organisation's network and extort victims with the threat of releasing stolen data. In 2017, over 30,000 individuals had complained of a data breach, with an estimated cost of \$77 million in the US alone⁶. High-profile individuals represent attractive targets to extortionists due to the perceived impact that publishing of sensitive data would have on their reputation and finances.



Case study – The DarkOverLord extortion group

The DarkOverlord is a group that threatens victims to release stolen personal and commercially sensitive information unless a ransom is paid. The group advertises its hacks on the darkweb, seeks media attention, and publicises well-known individuals compromised in data breaches to add extra pressure on targets.

In October 2017, the group stole sensitive customer data, including intimate photographs, from the London Bridge Plastic Surgery clinic and threatened to publish stolen images of several high-profile clients. The group has allegedly received over \$275,000 in extortion payments⁷.

Key recommended actions against cyber fraud

Key actions to mitigate the threat of extortion:

- Adequate backups and recovery strategy
- Training and awareness
- Endpoint protection

While these controls will contribute towards preventing common fraud attempts, a mature and resilient cyber security posture should include an all-encompassing cyber security implementation strategy. This remains true for the following sections as well.



4. europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

5. forbes.com/sites/geoffwhite/2018/09/26/how-the-dridex-gang-makes-millions-from-bespoke-ransomware/#6d3a764440d3

6. fbi.gov/news/stories/2017-internet-crime-report-released-050718

7. cyberscoop.com/dark-overlord-arrest-serbia/

Fraud



Business email hack

Scammers have attempted to impersonate businesses for financial fraud since well before the digital era. However, computers and emails have made a type of computer-enabled fraud called business email compromise (BEC) particularly prevalent due to its ease. In BEC, fraudsters mimic the email address or hack into the email account of a trusted colleague or client to impersonate them and defraud victims of large sums, often millions of dollars.

Organisations that often authorise large transactions are particularly targeted. BEC scams accounted for estimated losses of \$12.5 billion globally between October 2013 and May 2018⁸.



Case study – International BEC ring targets wealthy individuals

In June 2018, law enforcement officials arrested 74 individuals in the US, Nigeria, Canada, Mauritius and Poland, and recovered about \$16.4 million stolen via BEC scams. Some of the group's scams targeted high net-worth individuals and those who regularly transferred large amounts of money or sensitive records in the course of their business operations⁹.

Social media account hijacking

For those who have a family business that is publically traded, content posted on social media by high profile individuals or organisations can have a significant impact on their equities' value. Investors often monitor public social media profiles of individuals within the highest levels of an organisation to gauge insight on whether to sell or buy specific stocks.

A threat actor with temporary control over a high profile individual's social media accounts could post bogus information to modify stock prices of the listed entities linked to the victim. They could also publish content of private messages or attempt to ruin their reputation with defamatory information.



Case study – AP Twitter hijack causes \$136 billion market loss

In April 2013, hackers hijacked the Twitter account of the Associated Press (AP) and posted a fake message claiming that an explosion injured then US President Barack Obama. The hack was quickly discovered, and the compromised account suspended. However, in the three minutes following the fake tweet, panicked market reaction erased \$136 billion in equity market value, according to the Washington Post¹⁰. Although the incident affected a media organisation, it shows how quickly markets can react to fake news posted online by hijacking social media accounts.

Key recommended actions against cyber fraud

Key actions to mitigate the threat of fraud:

- Training and awareness
- Authentication
- Cyber threat intelligence



8. [ic3.gov/media/2018/180712.aspx](https://www.ic3.gov/media/2018/180712.aspx)

9. [justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals](https://www.justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals); [fbi.gov/news/stories/international-bec-takedown-061118](https://www.fbi.gov/news/stories/international-bec-takedown-061118).

10. [washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?noredirect=on&utm_term=.86e3b75b5da3](https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?noredirect=on&utm_term=.86e3b75b5da3)

Espionage



Cyber espionage involves sophisticated groups stealing data for political or commercial motives. Criminals, for instance, do it for insider trading or as hackers-for-hire for competitors¹¹. Family offices can have significant stakes in third party companies, while their owners often have political relevance. This means that individuals and their family offices are likely targets for cyber espionage, whether commercially or politically motivated. Stolen sensitive data could be used by hostile governments for surveillance or even to publish perceived embarrassing information.



Case study – North Korea, Russia target hotels' WiFi

Espionage groups compromise hotel Wi-Fi to target high-profile business travelers. The North Korean DarkHotel group compromised networks of hotels in Asia and the US since at least 2007, while the Russian APT28 group has done so in Europe and the Middle East. Family offices should safeguard information related to travel locations of high net-worth individuals to hinder targeting attempts.

Key recommended actions

Key actions to mitigate the threat of espionage:

- Endpoint protection
- Secure by design
- Firewalls and content security

However, sophisticated threat actors can only be countered with a mature and resilient cyber security posture that include an all-encompassing implementation strategy.



11. [fireeye.com/current-threats/threat-intelligence-reports/rpt-fin4.html](https://www.fireeye.com/current-threats/threat-intelligence-reports/rpt-fin4.html)

Cyber-enabled physical threats



Information gathering and unwanted attention

The information openly available online and from social media can reveal a significant amount of personal details that could be used to harass individuals or endanger their safety. Paparazzi can use public posts to harass high profile individuals. Threat actors can use access to information about friends and family, contacts, travel plans and current activities to plan a physical attack to an individual's safety. Threats to wealthy individuals have already been caused by incautious use of social media, such as family members sharing on social media the exact location of residence while abroad¹².

Vehicle compromise

Private jets, super yachts, and cars are targets due to their increasing reliance on connected devices. Modern yachts are particularly vulnerable¹³. Successful compromise can allow threat actors to take control of the engine and navigation systems. In at least one case, a cyber intrusion led to a full compromise of a superyacht, while GPS spoofing is increasingly prevalent¹⁴. High value cars also represent potential targets, although real-life exploitations have so far remained limited to keyless car theft¹⁵.

High value homes and estates compromise

Internet of things devices are increasingly present in high value homes. A 2015 study discovered that all the internet-connected security devices surveyed contained significant security vulnerabilities that would grant remote control of the device. The impact could be severe. Weak internet-connected security systems could be bypassed to facilitate physical burglary, or footage from security cameras hacked and posted online.

Key recommended actions:

Key actions to mitigate cyber enabled physical threats

- Secure by design
- Threat monitoring and penetration testing
- Authentication



12. campdenfb.com/article/market-insight-critical-risk-extortion-blackmail-and-kidnap-ransom

13. kaspersky.com/blog/yachts-vulnerabilities/21576/

14. boatinternational.com/yachts/luxury-yacht-advice/why-cyber-crime-is-the-biggest-threat-to-superyacht-security—33945 ; newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

15. express.co.uk/life-style/cars/1048780/car-theft-keyless-entry-hack-stolen-seconds-UK-epidemic

16. hp.com/us/en/hp-news/press-release.html?id=1909050

Key Recommendations

This section provides a brief summary of the top ten key controls that family offices and those they serve should prioritise in order to most effectively mitigate the cyber threats highlighted above. While some can be implemented in-house, others are more frequently outsourced by family offices to specialist providers for effectiveness and cost efficiency.

Preparedness

1. **Asset management** – understand the digital assets that are most critical to supporting your family and their wealth. Their classification enables prioritised and appropriate protection, monitoring and response strategies.
2. **Cyber threat intelligence** – ensure that you commission a service to monitor online open and closed sources. This could identify early warnings of potential threats, and indicators that an attack may have already been successful.
3. **Adequate backups and recovery strategy** – a technical solution should be in place to store and preserve the integrity of data backups. The solution should be tested, and recovery rehearsed to ensure it works.
4. **Training and awareness** – use active training and credible material to ensure staff are aware of the threats, how to prevent and detect them, and why it is important to do so – getsafeonline.org is a good source of material for internal training.

System and network security for protection

5. **Endpoint protection** – like medical check-ups detect potential health issues in your body, anti-virus software prevents and detect malicious activity in your IT systems. Make sure to maintain it always up to date.
6. **Authentication** – your house has strong locks and unique keys, so should your digital life. Always use strong passwords, restrict the use of administrator rights in your network, and protect important accounts with multi-factor authentication.

7. **Secure by design** – buildings must be designed for safety, so should your IT network. Ask your IT provider if they do configuration hardening, network segmentation, vulnerability management, and automated patching. These help minimise what attackers can exploit.

8. **Firewalls and content security** – like fences around buildings, firewalls protect your digital systems. Invest in firewalls and web proxy technologies to help detect and prevent potentially malicious network traffic trying to infiltrate your IT systems.

Managed detection and response

9. **Threat monitoring and penetration testing** – Test your IT environment for potential weakness that attackers could exploit, and use monitoring technologies to detect behavioral anomalies in computers and networks. This will help identify indications of attacks, facilitate an early response, and minimise possible impacts on the family, their assets or wealth.
10. **Incident response planning** – use of retained expertise to assist in planning, rehearsing and responding to any anticipated or actual cyber incidents and attacks.

Many security controls, technologies and practices are available to help establish a resilient posture. The top ten strategic controls above are considered key and, when implemented correctly and in combination, can provide a robust cyber defense capability. This will enable family offices to proactively predict and protect against known threats, while remaining vigilant and adequately prepared to detect and respond to new and emerging ones.

Key Contacts



Phill Everson

Partner, Cyber Risk Services Risk Advisory
+44 (0)20 7303 0012
peverson@deloitte.co.uk



Tim Erridge

Director, Cyber Risk Services Risk Advisory
+44 (0)20 7303 3872
terrige@deloitte.co.uk

Suspect you may have been victim to a cyber attack?

Call our 24/7 incident support line on **+44 (0)20 7007 9660**

or via email: **cirt@deloitte.co.uk**

Deloitte.

Private

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

Deloitte Private is the brand under which certain professionals in the Deloitte Network provide services to privately owned entities and high net worth individuals.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2019 Deloitte LLP. All rights reserved.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000
Fax: +44 (0) 20 7583 1198.