Family Offices & Privacy: A shield and a sword

Contents

1. Introduction

Robert Mueller, then director of the FBI, famously said in 2012, 'there are only two types of companies: those that have been hacked, and those that will be'.

Wealthy families have always been ripe targets for thieves and vandals, and the rise of the internet and electronic tools opened additional avenues for such criminals to operate — often with a cloak of anonymity.

The issue is serious, the threats are confusing, and advice for dealing with the threats is often unrealistic. Ask a technology consultant which criteria should be used for passwords, and you are likely to hear something similar to this: *Use a unique, 16-character password for every site and tool, do not use any known words in the password; include a mix of uppercase and lowercase letters, numbers, and special characters; never write it down; and change the password every 30 to 90 days*.

Considering that many of us have 25 or more such passwords, we are not able to follow these stringent guidelines. This Briefing Note considers the privacy risks and challenges for family offices, describes the most common risks they face, and offers a measured approach to address the challenges.

Our recommendations:

1. *Make privacy a **board or head of family level issu**e and do not leave it to the IT department*
2. *Invest in establishing a **human firewall** which will strengthen a family office's first line of defence against a cyber-attack*
3. *Be interested in **publicly available data** and correct inaccuracies or remove untrue information*
4. *Draw up an **incident response plan***
5. *Add **reputation and crisis management** to your incident response plan: in the event that your data is stolen as part of a cyber-attack, there are things you can do to minimise the fall-out. If the stolen data is leaked online, don't assume the battle is lost*

For information and advice on data protection, cyber security, and privacy contact:

TONI VITALE
Partner, Head of Regulation, Data & Information
020 3735 1934
tvitale@wslaw.co.uk

What is a 'human firewall'?

The key to preventing security breaches lies in raising awareness of employees to such a level that they become a line of defence in their own right – in essence, a human firewall. Increasing awareness has three elements: education, testing & governance:

- ***Education** - training should be given to new and existing employees. Threats constantly change so training should be ongoing, not a one-time event*
- ***Test** awareness to ensure this is improving. For example, create mock emails for employees to click on a link*
- ***Governance** - Put rules in place to:*
  - *ensure passwords are strong and changed regularly*
  - *limit access – only those that "need to know" can access sensitive data*
  - *clarify processes – whether someone loses a mobile device or receives a suspicious email, they should know who to call and what steps to take*

2. What types of risks are there?

One of the greatest risks to organisations is anticipating and planning for human behaviour. If your network security is onerous and not user friendly will your staff just pop down to the local coffee shop to use its free Wi-Fi?

Why should a family be concerned about potential cyber intrusions? At its core, there are three key concerns:

A. **Theft**: Someone might access bank, credit, investment or other financial accounts. Even if the family does not use online banking, their money may be at risk through phishing attacks, automatic teller machine (ATM) fraud or someone accessing their information through covert activity such as 'blagging'.

B. **Privacy:** Hackers may harm the family reputation (or its business) by revealing details about wealth, while thieves may use information to plan a robbery or kidnapping.

C. **Maliciousness**: Hackers may access data or websites just to delete or destroy data, or perhaps to redirect users to a different website. This may cost the family privacy, in addition to the cost of repairing the websites.

3. Where do the risks come from?

A. Emails

Panama-based law firm Mossack Fonseca recently generated headlines for all the wrong reasons. Nearly eleven million documents held by the firm were passed to a German newspaper by a whistle-blower breaching the firm's email server. The documents contained potentially compromising information on high profile clients' tax planning.

Lessons learnt from the Mossack Fonseca incident include:

(1) Make sure you understand what third parties are holding data related to you and your affairs

(2) Be prepared: if such a third party suffered a data breach so that you or your organisation was thrust into the public eye, how would you respond?

(3) Don't underestimate the importance of emails. They often contain substantial data, making email systems an attractive prospect for hackers

(4) Many people take a less formal tone when writing emails, but care should be taken. A comment made in jest in a 'private' email could cause substantial problems if taken out of context in a public breach. Email comments may seem passing, but can create an indelible link with the name of an organisation or individual

B. Viruses and malware

Malware is a real and continuing threat to most organisations. Anti-virus software provides some control, but it is very far from perfect – don't assume that just because you have anti-virus software you are protected.

Viruses are often contracted by visiting an infected website or opening an unsolicited email attachment.

This is not solely due to careless users – some of the largest, most commonly used websites in the world have been hacked to deliver viruses.

Commonly, a virus will:

- open a door for hackers to access systems directly;
- encrypt some or all of the data, and demand a ransom to unlock this; and
- record the activity and data on a computer (for example, passwords and credit card numbers) and automatically pass these to someone outside the organisation.

What is ransomware?

A virus typically spread by a corrupted link in an email. Once a PC is infected, victims are unable to access their data until a ransom is paid

Most ransomware incidents result in hours of downtime or networks taken offline for up to 10 days. Moreover, the attackers may still hold any proprietary data they picked up

Ransom, blackmail, surveillance, shutdown, and data manipulation can follow a ransomware attack

Often those affected pay the ransom, but this should be given careful consideration as it may not end the security threat or provide access to the ransomed data

C. *Employees being 'helpful'*

We like to think of cyber security threats as being technical, difficult to perpetrate and somehow beyond our understanding. In reality, the most common threat is an employee misjudgement or mistake. For example:

- Employees emailing unencrypted sensitive data (holdings, bank account details and personal data) means that the email will be sent over a public network. Anyone able to intercept or copy that email will be able to read it all.
- Storing data on public cloud services or on personal email. Using public 'cloud' services to share information can be really efficient, but you often have no control over access to, or sharing of, that data once it's left your systems. It makes little sense to build a highly secure set of internal systems that heavily restrict access to data if your employees are going to use public cloud services to share it.

We recommend that all family offices should:

(1) educate senior management and employees on security threats and how to respond;

(2) design risk, policy, technology and standards environments to help ensure the business operates according to the office's risk appetite;

(3) implement process and technology 'assurance' which provides independent and timely information on your state of information security compliance; and

(4) manage your security operation, making sure you blend education, architecture and assurance in a way that is appropriate to the organisation.

D. *Laptops, Tablets, Mobile Phones*

Laptops, smartphones, tablets, routers and connected devices ranging from printers to refrigerators to cars can provide access points for cybercriminals.

Family offices should review each device at least once a year against the following questions:

(1) Is password protection enabled for each device?

(2) Is there virus protection and a firewall installed on each device, whether in the office or at home?

(3) Is the software current and routinely updated on each device?

Smartphones should have password protection activated, up to date software and not used over public Wi-Fi. However, thieves can use inexpensive tools to monitor and listen to calls. If family members are using phones in certain foreign countries, or if they are actively involved in confidential business dealings that may be targeted, then they should consider encrypted phone services.

Any device with online access is vulnerable, including connected devices in a smart home. E.g. a nanny-cam that can be accessed through the internet, door locks that can be opened with a smartphone, vehicles with built-in Wi-Fi, and air conditioners and other appliances that can be controlled online.

E. Online / Cloud

Many families have a cloud-based document storage tool, through a private family website or through a third-party provider, to allow family members and advisors to access shared documents. Such families also may use internet-based accounting systems.

Most banks, credit cards and investment firms provide data access via the internet. While such firms often are the most diligent to protect their clients' security, they still represent a point of vulnerability to the family, particularly if the family accesses such sites through insecure methods or uses easily guessable passwords.

Many families refuse to use cloud-based software or tools, based on the risk of someone hacking into the data. However, that may put them at greater risk of losing their data if there was a fire or disaster in the office. In addition, there may be more robust and efficient tools that are only available in the cloud. Most families want to balance their security with the capabilities and services that are available in the cloud.

F. Wi-Fi

Public Wi-Fi is one of the most common sources of breaches. When a family member logs into their email from open wireless access systems often used in coffee shops or hotels, thieves can intercept passwords as they are typed, along with pictures and data stored on the device. Many security experts tell families not to use public Wi-Fi under any circumstances. However, there are times where data service is not available or perhaps too slow. Using a Virtual Private Network (VPN) on top of the Wi-Fi is a relatively inexpensive solution that significantly increases protection.

Home and office routers are other points of vulnerability. Routers are often used beyond their "end of life," or the time where manufacturers stop issuing software updates for them.

Ensure Wi-Fi routers:

(1) have current software;

(2) are replaced every few years; and

(3) are password enabled and use robust passwords.

G. Other threats

Passwords are always a point of risk, whether to an email account, online banking or various websites. The more complex the password, the more likely someone is to write it down. A common security risk is to provide every staff member with a copy of a password sheet with the various online banking and other account passwords. Anyone accessing the office could easily copy the sheets each night, giving them full access to financial accounts.

Phishing is a method of defrauding someone by posing as a legitimate person or business. Most commonly, this involves sending emails to get recipients to log into a website and provide password or other confidential information. It might appear to be an email from your bank, or a package delivery company, with a link suggesting there has been fraud involving your account. Following the link may result in real fraud occurring, as you now provide the person your real login and password information.

Several years ago, these emails were more obvious as the spelling and language were poor, obviously written by someone not native to the UK. However, they have improved significantly in recent years.

Debit and credit card fraud - Some firms have discovered devices attached to an ATM, reading the card when inserted. Users receive cash as usual, but thieves now have their account information and password.

Questions to ask at your next board meeting:

1. *Have we ever suffered a cyber-attack, and if we have, what can we learn from it?*
2. *What monitoring is in place to detect an attack?*
3. *Have we ever independently tested our firewall using a penetration test and if so when?*
4. *What steps are we taking to strengthen our human firewall?*
5. *Who has what information on the family and where is that information going?*
6. *When did we last rehearse our incident response plan and are we clear on who will do what in a crisis?*

4. How to mitigate the risks

A. Train your staff

Training should

- adopt best practice policies to build awareness;
- be interesting, personal and real;
- cover new and existing staff;
- make it easy for people to report suspicious emails, a potential cyber-attack or other concerning behaviour; and
- clearly outline your company's cybersecurity processes.

B. Adopt the best applicable IT standards.

There are many 'IT standards' that can provide guidance and the challenge is often not whether to conform to a standard but which one to follow. Examples include:

(1) ISO27001 – Information Security Management

This is the primary standard for security. It can appear cumbersome and disproportionate to many organisations but, when applied by a skilled practitioner the standard can apply as much to a small family office as a multinational financial institution.

The heart of the standard suggests that:

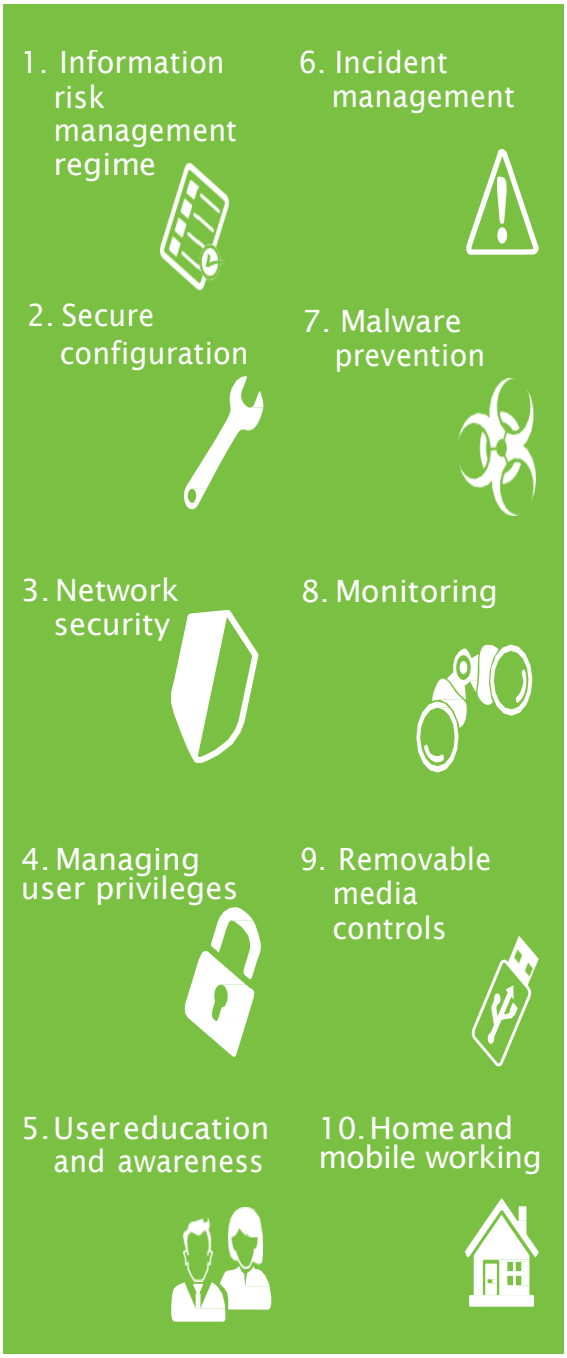
- security is a process, not a destination, and that to embed this process you need to (a) plan what you intend to do (b) actually do it (c) check it's working properly, for example through testing, auditing or ongoing monitoring and (d) act appropriately when you find it's not working properly;
- security is far more than technology. Both ISO27001 and ISO27002 offer target controls for technology, but also people, management, third party oversight, physical security and risk management.

(2) 'Top 20' Security controls

Both SANS and the UK 'centre for the protection of national infrastructure' (CPNI) maintain a list of 20 controls organisations should have in place to manage the cyber risk. While these are more technical in nature, applying a list of 20 controls can be more straightforward than finding a skilled practitioner to implement ISO standards.

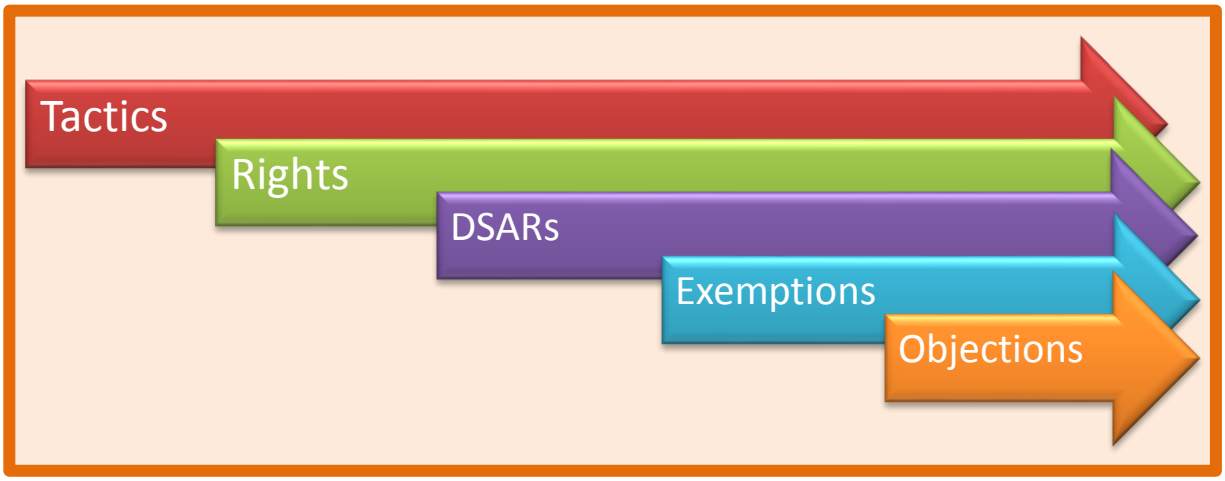
(3) 10 steps to cyber security

The UK Government offers practical guidance to help organisations manage the cyber security risk, through its '10 steps' organisations should take to help manage the cyber security risk. 'Cyber Essentials' also includes prepared board briefings and implementation packs to support the guidance. The scope ranges from 'information risk management' to more specific technical controls designed to mitigate many of the vulnerabilities that lead to people being hacked (such as firewalls and virus protection).



5. GDPR as a Sword – new tools to use proactively

The GDPR provides a new armoury of tools which can be used tactically by aggrieved data subjects. It will not always be possible to neutralise these tactics but family offices should be away of the new rights afforded to their principals and how to defend themselves if the tactics are used against them.



1) Data Subject Access Requests: Data subjects can legitimately request the following information (and their motive is irrelevant):
   a) Description of the categories of personal data;
   b) Purposes for processing data;
   c) Countries where data is stored, or accessible from, and to whom the data has been disclosed or may be disclosed;
   d) Retention period, or the criteria used to determine the period;
   e) Where the data comes from, if not collected directly from the data subject;
   f) Safeguards in place for sending data to a third country outside the EEA.

2) Section 10 DPA 1998 allowed individuals to prevent processing likely to cause distress or damage – the GDPR includes the right to object and restrict in much wider circumstances. An individual can object when data is processed for the public interest and where there is a legitimate interest. There will probably be good grounds for individuals to object and either restrict or erase.

   Breach notifications – data subjects may have to be notified of some breaches which may trigger legal claims.

3) 'Automated processing' now includes 'profiling' – this is defined as the evaluation of "personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

   The profiling definition is wider than the DPA 1998. Specific inclusion of these references will make it easier to bring a complaint to a company.

   Data subjects are entitled to receive meaningful information concerning the basis for the logic in making such automated decisions, and the significance and envisaged consequences for such processing.

4) The journalistic, literary and artistic exemption now includes academic as another basis for withholding data. However, the DPA 2018 also lists specific guidelines and codes of practice which must be taken into account (Sch 2 Part 5 para 26(6)), which is more specific than the 1998 Act.

   Third party rights exemption – a controller must take the type of information about a third party into account as well as other requirements – this may mean that they are obliged to reveal more than previously.

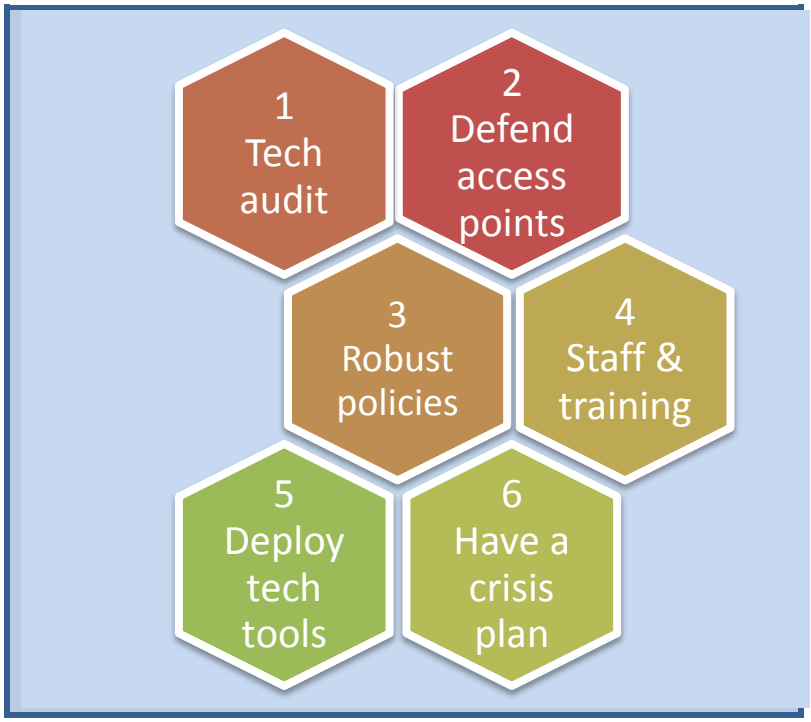
   The criteria are:
   (a) the type of information disclosed;
   (b) any duty of confidentiality owed to the other individual;
   (c) any steps taken to seek the consent of the other individual;
   (d) whether the other individual is capable of giving consent; and
   (e) any express refusal of consent by the other individual.

6. Password do's and don'ts

Password do's	Password don'ts
• Use unique passwords that combine words, numbers, symbols, and uppercase and lowercase letters. • Use different passwords for different secure sites. For sites that do not store financial or private information, you may consider a common password. • Change passwords regularly, even if the site doesn't require it. Changing every 60 days is ideal, but even a semi-annual or annual change is better than what most people do. • If you must write down a password, write just a clue or abbreviated form — something that only you can decipher. However, still don't leave the clue in obvious or easily found places. • While 12—15-character passwords are ideal, it is best to use at least 8 characters. • Consider a password utility service.	• Don't use your network name or email address as your password. • Don't use easily guessed passwords, such as "password" or "123456". • Don't choose passwords based on personal details, such as birthdates or family names. • Don't use dictionary words or names in their correct form. • Don't use the same password at multiple secure sites. Consider a common theme with unique twists. • Don't share your password online or over the phone — not even with friends or family. • Don't enter passwords to secure sites while using unsecure public networks, unless you are using a VPN.

7. Privacy Action Plan for Family Offices

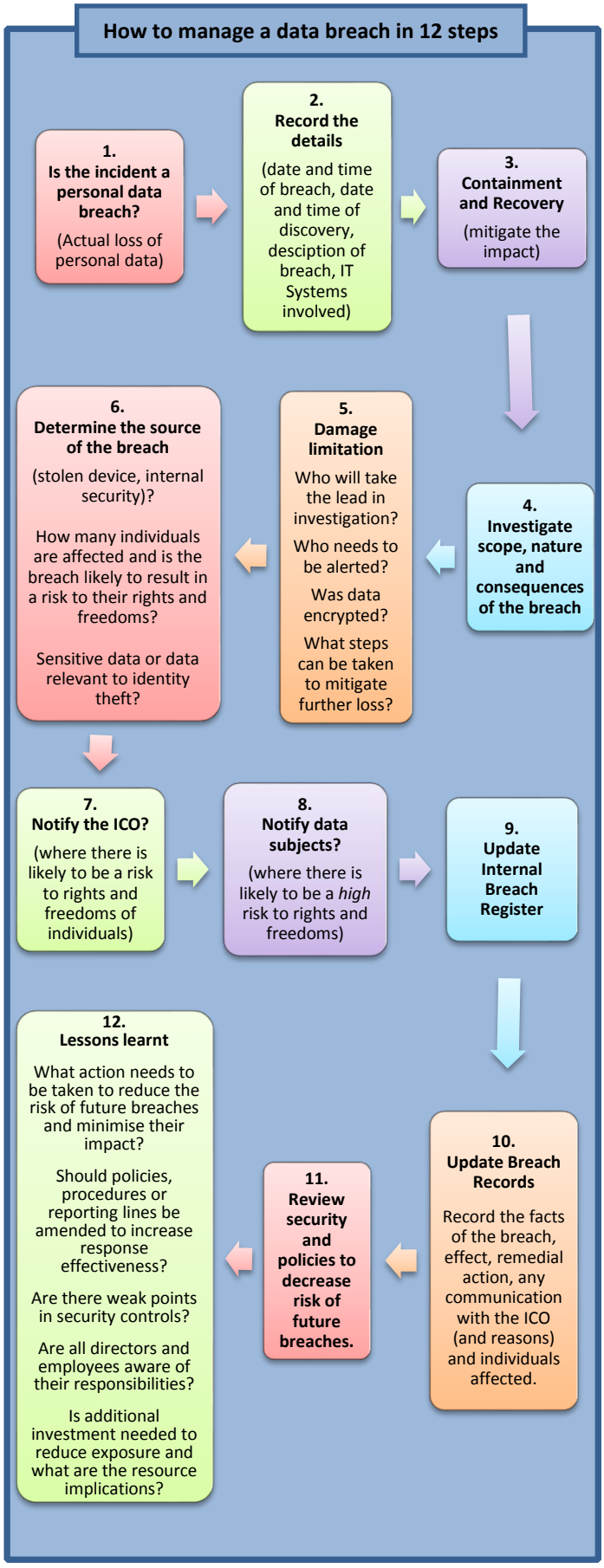
1. **Technology Audit** - List, monitor and track all laptops, smartphones, tablets, routers and connected devices ranging from printers to refrigerators to cars. Each device must have updated antivirus, firewall and similar software.
2. **Defend access points** - Monitor the family office network, business networks and family home networks, looking for signs of an intrusion.
3. **Robust policies** – Implement at least the following policies:
   - *Connected device policy* - describes use of Wi-Fi, VPNs and routers.
   - *Identity protection policy* - describes how the office protects the personal identity of each member.
   - *Social media policy* - explains how family members use social media.
   - *Password policy* - describes what the family decides is a reasonable standard for passwords, on phones, tablets, routers and similar devices.



4. **Staff & training** - Family offices should ensure they have current signed contracts with each vendor or company they work with as well as confidentiality agreements with all staff. As well as regular training the family office also should repeat background checks regularly on their own employees, along with household and other staff with access to family houses, offices and resources. Training should be refreshed regularly too.
5. **Deploy tech tools** – e.g.:
   - *Data backups:* multiple backups of servers, laptops and phones
   - *Vulnerability assessment:* have a technology firm conduct an annual vulnerability assessment
   - *Encryption tools:* use secure document storage, encrypted email tools
   - *Monitoring:* activity logs can be used to detect suspicious activity
6. **Have a crisis plan** - The plan should address:
   - lost phones or laptops
   - what actions family and staff should take if they receive a phishing email or phone call
   - how to handle a ransomware event, hacked emails and network intrusions
   - rehearsing your response to a cyberattack

20 Questions for your breach response plan

1. Who should be notified within the organisation if there is a data breach?
2. What happens if one of the team is away on holiday or absent? Is there a back-up plan?
3. Are there clear reporting lines and decision-making responsibility?
4. What specialist external assistance do you have lined up?
5. Is there a designated person(s) responsible for managing breaches?
6. What is the process for triaging incidents and activating the breach response team?
7. What are your contractual rights and obligations with third parties?
8. If you hold credit/ debit card data, do you need to notify your payment processor?
9. What are the potential liabilities?
10. Who should gather information about the breach including statements from staff?
11. How do you determine if the breach is notifiable to the ICO or the data subjects?
12. How do you secure and isolate IT equipment without destroying evidence?
13. Do you need to secure the physical security of premises?
14. Can you switch off staff access and change logons and passwords centrally?
15. Do you have cyber breach insurance which may cover a data breach?
16. Do you know what data is encrypted?
17. Are staff appropriately trained as to how to deal with data subjects in a breach scenario?
18. Do you have PR capability experienced in dealing with data breaches?
19. Do you have template pro-active and re-active press statements?
20. Can you actively monitor social media after a breach?



Our Regulation, Data & Information team

Toni Vitale
Partner, Head of Regulation, Data & Information
tvitale@wslaw.co.uk

Toni Vitale is Head of Regulation, Data & Information and has extensive experience on GDPR, data breach investigations, audit and policy implementation, binding corporate rules, international data transfers, DPIAs, security reviews, contractual reviews, consent, subject access requests and defending ICO complaints.

Jon Baldwin
Partner, Regulation, Data & Information
jbaldwin@wslaw.co.uk

Jon specialises in finding pragmatic, commercial and risk-aware solutions for companies operating in regulated sectors. Jon advises clients on state aid, data protection, freedom of information, financial and consumer credit regulation, and statutory powers.

Hannah Ife
Solicitor, Regulation, Data & Information
hife@wslaw.co.uk

Hannah joined the Regulation, Data and Information team in April 2018. Prior to commencing a career in law, Hannah spent four years working within the risk management team at a FTSE-100 international retailer. Hannah's recent experience includes assisting international companies in preparing for the GDPR.

Helena Parker
Trainee Solicitor, Regulation, Data and Information
hparker@wslaw.co.uk

Helena has previously worked as a temporary paralegal in Litigation for firms including MacFarlanes and Norton Rose Fulbright, and has undertaken work experience in the Private Client and Family departments for Crane & Staples. Prior to commencing her legal career she worked for a health technology start-up.

Robert Paydon
Partner
rpaydon@wslaw.co.uk

Robert is an experienced commercial litigation/dispute resolution and is particularly concerned with the protection and management of corporate and individual reputations, particularly through the law of defamation and privacy.

Louise Lawrence
Partner
llawrence@wslaw.co.uk

Louise advises clients on privacy and data protection issues involving service agreements, grievances and disciplinary issues, settlement agreements and departure situations.

Andrew Yule
Partner
ayule@wslaw.co.uk

Andrew works with clients across a range of sectors advising on privacy and data protection matters - at each stage carefully managing not only the financial terms, but also the more nuanced reputational aspects.

Theresa Kerr
Senior Associate
tkerr@wslaw.co.uk

Theresa specialises in the education sector and advises on a range of issues including data protection, freedom of information, governance and contracts. Theresa's clients include all types of schools including maintained schools, special schools, academies, large and small multi academy trusts and umbrella trusts.

Services available from Winckworth Sherwood

1. **Helplines**
   - **GDPR General Helpline** – To deal with ad hoc queries and questions.
   - **GDPR Emergency Data Breach Helpline** – Assisting in the immediate aftermath of a data breach, advising as to whether the breach is reportable and the steps you should take in the first days after the breach.
   - **ICO Investigations Helpline** – Advising you as to how to handle an ICO investigation, what to say and what not to say and how to mitigate the potential sanctions against you.
   - **DSAR Helpline** – assisting with data subject access requests: Including preparing response letters and redacting material to apply exemptions.
2. Drawing up a bespoke **Action Plan.**
3. Preparing board briefings, analysis, reports and updates.
4. **Training** – including training your Data protection Officer in aspects of the role including soft skills and board level reporting and how to deal with the media.
5. Undertake **periodic data protection audits** to assess compliance with data protection requirements and produce an Action Plan to ensure any deficiencies identified as a result of an audit are addressed.
6. Carry out **Data Protection Impact Assessments.**
7. Review policies related to Data Protection such as Information Security, Social Media, Crisis Management.
8. Conduct **risk assessments** on data protection compliance at appropriate intervals.
9. **Maintain a central register of data security reports** in a form that allows you to:
   - monitor and assess the effectiveness of the data protection systems
   - identify any data security report or other information that may be linked
   - adequately respond to requests for information
   - identify any training needs
10. **Advice on incident management**
    - How to respond to and manage (including liaising with the ICO and any other regulator) any:
      - data security breaches
      - data security reports
      - communications received from or enforcement action initiated by the ICO or any other relevant regulator
      - complaints or communications relating to data protection and/or security received:
        - from other professional representatives .
        - directly from clients and other members of the public.
11. **DPO support services** – assisting your Data Protection Officer or team to:
    - Guidance on DPO role specification
    - Raise data protection awareness and advising on GDPR compliance.
    - Ensure the implementation of the appropriate documentation to demonstrate GDPR compliance.
    - Monitor the implementation and compliance with policies, procedures and GDPR in general.
    - Handle data breaches, including notification to the ICO and data subjects.
    - Liaise with the ICO, the employees' representatives and with the data subjects.
    - Cooperate with and acting as the contact point for the ICO 'on issues relating to processing'.
12. **Policies & document reviews**:
    - Reviewing policies, terms and conditions, purchase orders, contracts and notices to ensure GDPR compliance.