Law Society of Scotland

Guide to cybersecurity

2nd edition 2019

In association with

MITIGO CYBERSECURITY

Introduction

Cybercrime and information security present challenges for all organisations. A cyberattack or data breach can cause major disruption, reputational damage and financial loss.

Year on year, an increasing number of businesses have been affected by frauds and scams, with many high-profile data breaches. The UK Government's 2018 annual survey found that 43% of British businesses experienced a cybersecurity breach or attack during the year.

Professional service firms, such as law practices, are at particular risk because they hold large amounts of detailed personal and commercial data, often combined with the movement of significant amounts of money. The consequences of an attack can be severe and may include a breach of client confidentiality and regulatory compliance. Recent figures show that the most severe breaches can cost small to medium-sized businesses more than £300,000.

This guide outlines some of the key threats and provides basic tips for best practice.

What type of information should you be concerned about?

In developing a security strategy, you should consider all types of information. And in all forms – emails, databases, text documents, spreadsheets, voicemail messages, pictures, video and sound recordings. Also, the risk exists whether held on your own systems and devices, or on third-party hosted systems, such as the cloud. Consider:

- **Solicitor-client data**
- **Personal information about people, such as names, addresses, national insurance numbers, ethnicity, bank account details**
- **Staff information**
- **Company private information, such as intellectual property for products and designs**
- **Financial data and financial transaction records**
- **Tax records**
- **Details of proposed business deals**
- **Company growth strategies**
- **Proposed legal action**

Risk areas

This is a high-level summary of the top areas where cybercriminals will look for vulnerabilities to exploit:

Computers and IT systems

A firm's computers, servers, storage, phones and network are all vulnerable to cyberattacks. Issues occur when the network has not been properly secured and the security settings on devices are not configured correctly.

Your staff and contractors

Without proper training staff can be your most significant vulnerability. Cybercriminals will exploit staff who do not think before clicking on weblinks, email attachments and even social media videos. Passwords in the workplace may be weak, re-used and shared as staff prioritise convenience over security. Insider threat from unhappy staff is also an issue if policies and procedures are not effective.

Personal mobile phones and devices

Personal devices such as phones, tablets and laptops are increasingly used for work purposes, especially for the mobile workforce. These are easier to attack than corporate IT equipment, which often has more restrictions and protections. Personal mobile phones may be allowed to connect to the office Wi-Fi, which can provide cybercriminals with access to critical data and information.

Remote and home working

Staff working remotely, when travelling or at home, are more inclined to make compromises on security by using personal email accounts, insecure connections, personal social media accounts and browsing unrestricted websites.

Cloud portals and platforms

It is increasingly common for law firms to use cloud portals and platforms provided by third-party software suppliers for document management and practice management. This can become an exploitable vulnerability if supplier due diligence is not thorough and security configuration is not applied and maintained.

Data transfer and storage

Transferring data as an email attachment creates an exposure risk and relaxed access management rules mean that personal data is easily found on networks. Firms may unconsciously allow staff to use cloud services to transfer information. Dropbox, Gmail, and Hotmail, for example, are cloud services that employees may use to transfer information.

A firm's public website

Your public-facing website is often a target for cybercrime. Examples of breaches include a denial of service attack, which takes the site down completely; a hack into systems that sit behind the website, such as customer databases; and, the insertion of spyware to intercept customer information.

Client accounts and cashroom

Any area of a business that handles money and bank account details is a target for cybercriminals.

The threats

INDISCRIMINATE

Indiscriminate attacks seek to exploit human error or common technical vulnerabilities in systems and websites. These attacks are frequent and target as wide an audience as possible. So, businesses large and small become targets.

TARGETED

More specific targeted attacks often follow on from indiscriminate attacks where a vulnerability has been discovered and is then exploited in a more focused manner.

Targeted attacks can also occur when cybercriminals acquire information about your business or your employees (for instance, from social media or the dark web) in order to tailor an attack.

They may also originate from disgruntled employees who are after specific information or other asset.

The threats

The more common threats are:

Email phishing

This type of attack is generally received via emails that appear to come from a legitimate organisation, for instance, a bank or one of your clients or suppliers. The emails contain a link to a fake website that replicates a real one. The victim is then encouraged to input sensitive information, such as passwords. Typically, poor phishing attacks have bad spelling or grammar within the email. For those that look more professional, the only real giveaway is the fact the email asks the victim to click on a link.

SMS phishing (smishing)

Smishing involves sending a fraudulent link via text message to a mobile phone. This can be very effective as staff are generally more likely to click on text message links. There may also be fewer clues to look for in a short text.

Voice phishing (vishing)

Here, the victim receives a phone call from someone claiming to be from a legitimate organisation, eg a bank's fraud unit. The caller may know the victim's name and account number, often asking for the head of finance or head cashier by name. The caller display can even show the correct bank phone number if the fraudster has created a false number. The caller will warn about possible suspicious activity on the bank account and might even be able to give genuine details of recent transactions. The fraudster will then claim that the account has been frozen due to suspect transactions but that payments can be made with their assistance. The victim is then persuaded to either provide details of passwords and account details or transfer a sum of money directly to the fraudster to overcome the problem. Sometimes the fraudster will keep the phone line open and advise the victim to call their bank, remaining on the line without the victim's knowledge during the call.

Social engineering

Humans can be the weakest link in cybersecurity, and attackers use freely available information to pick out who is likely to be vulnerable. Information from social media, such as Twitter, Facebook and LinkedIn, can be very useful as people often discuss events and changes in their work and public life. The telephone is the most common form of social engineering. Attackers often use social engineering techniques, such as pretending to be IT support staff, to con users into giving away their passwords and then using those to access the system.

Email spoofing

The email of a firm's senior leader is often readily available on the internet. A common cyber-fraud involves sending an email to the firm's accounts team, from the CEO or senior partner, requesting an urgent and immediate payment to a new account. The email address replicates that of the CEO, resulting in more junior staff feeling obliged to make the payment quickly and without question.

The threats

Invoice hijacking

This scam involves a fraudster intercepting correspondence between two parties who have an existing contractual relationship. The fraudster then invoices the target for services that have actually been rendered. Typically, the client receives an email asking for funds to be transferred to a separate account, perhaps “due to a limit being reached”. The fraudster provides details of a new account to which the client sends the funds. This fraud will often rely on email correspondence being hacked, leading to disputes as to who was at fault. Invoice hijacking inevitably damages client relations and may cause reputational harm.

Malicious software (malware)

This is any piece of software that is specifically designed to disrupt or damage a computer system. It carries out a hidden function on the target system for an attacker and comes in many different forms, such as ransomware, Trojans etc. Commonly installed alongside quasi-legitimate software, malware can also be disseminated via email attachments, web browsing and file sharing. Once malware is on the system, it can be difficult to detect and remove.

Ransomware

This is a type of malware that infects a computer or network, blocking the victim from some or all of a system/data. A sum of money may be paid to the criminals, who then send the victim instructions on how to unlock the data.

Virus

A virus is malware that, when executed, reproduces itself (copying its own source code), infecting other computer programs by modifying them.

Trojan

A Trojan is designed to damage, disrupt, steal, or inflict some other harmful action on your data or network. A Trojan acts like a genuine application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the intended damage.

Malvertising

This malware exploits vulnerabilities in frequently visited websites. The websites are hacked and then used to deliver malicious software to website visitors through adverts and downloads.

Website and network hacking

Hacking involves someone trying to remotely access a business or personal IT system, using a variety of widely available tools and known vulnerabilities. Hackers target online services and IT systems to steal, corrupt or destroy information.

Distributed denial of service (DDoS)

DDoS involves either interrupting or shutting down a target IT system by flooding it with requests, for instance, external emails. The target system is unable to respond effectively to the high volume of traffic and slows or shuts down. A DDoS attack commonly targets large services, such as email and websites, which has a follow-on effect on smaller entities.

The consequences of a cybersecurity breach

The information created and processed by a law firm is one of its most valuable assets. The consequences of a cybersecurity breach could be:

Financial loss

Firm funds could be stolen, and loss of income could result from inability to operate, failure to complete client work or business deals, reduction in productivity, staff downtime, increased insurance premiums and the cost of attempting to recover lost information, equipment or data.

Reputational harm

Clients expect their solicitor to work to high standards in a safe and secure environment. A security breach will cause reputational damage and could result in loss of existing and potential clients.

Breach of legal obligation

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 require appropriate technical and organisational security. Non-compliance can result in fines, enforcement notices, or an investigation from the data protection regulator, the Information Commissioner's Office. Regulatory fines for non-compliance can be up to either 4% of annual global turnover or €20 million. See the Law Society's *Guide to GDPR* for more information.

Breach of contract

Solicitors working under panel appointments, for example with banks or public bodies, may find themselves in breach of contract and potentially liable to indemnify their clients if a security breach results in a data loss.

Breach of professional rules and standards

Protection of confidential information is a fundamental feature of a solicitor's relationship with clients under the Law Society's practice rules and standards of conduct. Failure to introduce satisfactory security measures could be seen as a breach of this obligation and lead to a finding of misconduct.

Solutions ~ tips for individuals

Total security can never be guaranteed but following these basic steps will help to prevent many cyber-breaches. Cybersecurity is not simply an IT issue, it is a boardroom issue; and a security culture should be instilled among all staff.

Digital usage and behaviour

Changing digital behaviour at work is key to reducing the risk of cybercrime. Individuals must learn to pause long enough to question whether the action they are about to take may be unsafe.

Phone calls

Never accept at face value a caller who asks for financial or confidential information. If you receive a call claiming to be from your bank, politely end the call and then contact the bank yourself on a different telephone line. Always use an official bank number. Do not use a number that the caller has given you. Remember that the major UK banks have made declarations that they will never: ask you for your PIN or your online password; ask you to withdraw money to hand over to them; ask you to transfer money to a new account for fraud reasons; send someone to your place of work or home to collect your chequebook, cash or payment card.

Web browsing

When browsing the internet, staff should always be wary of bogus websites and leave the site if in doubt. For example, if you become suspicious of a site because the wording on the site is incorrect or the site address seems strange, you should leave. Use software on your IT system that gives warnings about known malicious internet sites.

Social media

Think before you send a tweet or issue a post on social media that could compromise you, your firm or a client. When clicking on adverts, videos and links, consider if the source is safe and whether you should be doing this on a business device.

Receiving emails

When receiving emails, think before you click on links or open attachments from addresses that you do not recognise. Look at the sender's email address and ask yourself:

- Do I know this person and is this their usual email address? Fraudsters do attempt to send emails using legitimate email addresses. They may have obtained these email addresses from contact lists using malware installed on the computers of family, friends or colleagues.
- Does this email subject look unusual? Out-of-the-ordinary or poorly written subject lines may hint at a fraudulent or spam email.
- Is there an attached document and do I recognise the attached format (Excel, Word, PDF etc)? Be wary of zip files if you are not expecting to receive them. Does the email mention the attachment and am I expecting an attachment? Attachments can transmit malware, so open them with caution. If you receive an email with attachments that you are not expecting, try, as far as is practicable, to contact the sender and check if they have sent an attachment. Attachments from emails can be saved to folders without opening them. These folders can then be scanned with anti-virus software before they are opened.
- Does the email ask me to visit a website, send personal information or reply immediately? Be particularly wary of emails that request personal information, particularly banking details – banks will never ask you to disclose your password in an email. Some emails may state that you need to reactivate your account due to maintenance, or your computer contains malware and needs to be cleaned. Do not respond to these requests. Never provide your username or password in response to an unsolicited email.
- Am I being asked to click on a link? Be wary of links in emails – they can easily be disguised and may take you to malicious websites. If in doubt, do not click on the link but hover your cursor over any addresses or links in an email and check if text appears – this is often an indication that something is amiss. Always go directly to a website rather than follow a link within an email.

Personal mobiles and laptops

Only use a personal device for work purposes if it has been approved by the business. Personal devices used for work should have a strong password to unlock and, as a minimum, use active anti-virus software and the latest operating system. Personal mobile devices should be connected only to guest Wi-Fi and not to the firm's secure network unless specific approval has been received.

Software updates

Do not ignore or delay the regular software updates that your computers and mobile phones receive as they always contain important security updates. These updates include the operating system that runs your device and the applications you use to do your work.

Virus/malware protection

Do not ignore alerts from your anti-virus software; they are designed to warn you when something is a risk. Read pop-ups carefully and take the appropriate action.

Solutions ~ tips for individuals

Password and access management

Reducing access to important information stored on a firm's systems is a key cyber defence. If a cybercriminal gets access to the network, documents and information may still be safe if access to the storage folders is limited to named individuals and sensitive files are protected with strong passwords and encrypted.

Password policy

Traditional advice is that an obscure password with a mix of capitals, special characters and numbers is best, and that you should change it frequently. But there is an increasing preference for simpler and more memorable password phrases that are much longer. If you are using a password management system, ensure that it is robustly protected with a secure and strong password.

There is a tendency to share passwords in the office due to confidence in colleagues and convenience. Passwords should never be shared or left on display.

Access management

Make sure you lock your computer when it is unattended to prevent unauthorised access.

Confidential data should be saved in files and drives that have been set up to restrict access to a named audience.

Remote and home working

When working on the move, information becomes more vulnerable. Use your common sense. Be aware of your surroundings and of how information could be compromised.

- Avoid transferring confidential or sensitive data over public Wi-Fi networks – the information sent over free networks offered by trains, hotels and coffee shops can be easily compromised.
- Using remote devices on public transport – be vigilant and make sure the screen of your laptop, mobile phone or other device is not visible to others. Work tidily and with care. Ensure that no information is on display.
- Personal IT equipment – make sure your employer approves the use of any personal IT equipment, and you comply with their security requirements, such as ensuring that software is up to date, and includes anti-virus protection and a firewall.
- Wireless network – if you have a wireless network, ensure that it is secure, using the recommended settings and latest encryption software, and that only authorised users can connect to it.
- Social media – use privacy settings to control what information you share over social media.
- Mobile phones – when dealing with sensitive information over the phone, be aware who might overhear, purposely or not.
- Beware of insecure networks – web-based email accounts are particularly risky. Avoid using personal email addresses to send confidential information. Always check and comply with your firm's policies.

Information transfer, handling and encryption

The transfer of data between companies and individuals can be vulnerable.

Emails

It is easy to become complacent about emails because they are so familiar, but users should not rely on their emails remaining private. If you are sending sensitive or confidential information by email, it should be encrypted.

When sending emails to external addresses ask yourself:

- Are you allowed to share this information with the addressee?
- Is it personal or confidential information?
- Can the information be sent openly, or does it need to be protected?
- What kind of protection would the email require?

Cloud platforms

When sharing documents through a cloud platform, such as Dropbox or Google Drive, do not use personal accounts. Also, make sure you have the firm's approval to use this method. Follow the firm's policy on how long that information can be stored on that cloud location.

Removable storage devices

When using removable storage, such as a USB drive, ensure you have the firm's permission to do so. The drive should be used in line with the firm's policy with consideration given to, for example, password encryption, scanning the drive with anti-virus software and the drive should be wiped after use.

Solutions ~ tips for firms

Risk-based assessments

Undertake a proper and thorough risk-based assessment of your firm's information security requirements. You are legally obliged to do so in respect of all the personal data you hold. Take steps to make information security part of your normal business risk-management procedures. Disseminate key security principles among your staff to ensure they become part of your firm's culture.

Asset audit

Carry out an audit of any assets that are potentially at risk – identify financial, personal and other information assets that are critical, and the IT services you rely on.

Vulnerability assessment

Undertake an assessment of your cybersecurity resilience and identify where you may have vulnerabilities and take appropriate remedial action. Assess all the IT equipment within your firm, including mobile and personal IT devices. Understand the technical and organisational risks to these and how these risks are currently managed.

Expert advice

Decide whether you need to seek expert advice and assistance to undertake the risk and vulnerability assessments, and to get the right security controls in place for your firm. Regardless of whether your IT is out-sourced or inhouse, it is useful to get external expertise.

Risk framework and governance

Put in place technical and organisational measures to satisfy the security obligations relating to personal data and to control the risk of cybercrime. Monitor their effectiveness on an ongoing basis.

Senior accountability

The senior management team should take ownership of this risk and track it at the firm's partnership meetings. Appoint a senior member of staff to oversee data and cybersecurity. Ensure they have the right resources and support to do this job.

Cybersecurity policies

Prepare and issue clear policies on all key aspects of data and cybersecurity. All staff should be made aware of their security obligations and the policies that apply to them. These should include, for example: policies on the use, by staff, of business internet facilities for their personal matters; use of social media; and, policies on bring your own device (BYOD).

Monitoring and review

Review your systems and procedures regularly and respond to any changes or problems you identify, including attacks or disruption to your firm.

- Ongoing monitoring – test, monitor and improve your security controls regularly to manage any change in the level of risk to your IT equipment, services and information.
- Disposing of programs or physical devices – remove any software or equipment that you no longer need, ensuring that it contains no sensitive information.
- Managing user access – review and manage any change in user access, such as the creation of accounts when staff members join the firm and deactivation of accounts when they leave.

Incident management

If your firm is disrupted or attacked, carry out a post-breach review. Your response should include: removing any ongoing threat, such as malware; understanding the cause of the incident; and, if appropriate, addressing any gaps in your security that have been identified following the incident.

Record keeping

Keep appropriate records. This should include details and evidence of: your risk-based assessments; the technical and organisational measures taken to protect the security of personal and client data; your processes for testing, assessing and evaluating the effectiveness of those measures; and, cyber-incident management.

Accreditation

The ISO27001 standard is a specification for an information security management system. This will require significant levels of IT governance. As a minimum, you should get Cyber Essentials certified. However, be aware that this does not cover other necessary organisational measures, such as training and policies.

Solutions ~ tips for firms

Steps to cybersecurity

Firms should take a number of steps firms to become cybersecure.

Computer network security

Protect your networks, including your wireless networks, against external attacks by using firewalls, proxies, access lists and so on.

Maintain an inventory of all IT equipment and software. Identify a secure standard configuration for all existing and future IT equipment used by your business. Change any default passwords.

User awareness and training

Education, which can take many forms, is at the heart of understanding the scope and breadth of data protection. Ensure that your staff have read this guide and have received appropriate awareness training, so that everyone understands their role in keeping the firm secure. As well as explaining procedures, the training should incorporate advice on the risks the systems are designed to avoid and their potential consequences.

Malware prevention

Install anti-virus solutions on all systems and keep your software and web browsers up to date.

Removable media

Restrict the use of removable media, such as USB drives, CDs, DVDs and secure digital cards, and protect any data stored on such media to help stop data being lost. Scan all media for malware before importing onto corporate systems.

Encrypt sensitive data

Ensure that sensitive data is encrypted when stored or transmitted online so it can only be accessed by authorised users.

Secure configuration

Many security safeguards will be built in to your computer systems, including anti-virus software, algorithms that check for unusual activity, automatic back-up and so on. Ensure that your IT systems are fit for purpose. Take steps to put security controls in place for your firm. If you use third-party-managed IT services, check your contracts and service level agreements, and ensure that whoever handles your systems and data has these security controls in place.

Managing user access and privileges

Restricting access to inappropriate websites will lessen the risk of being exposed to malware. Create a policy governing when and how security updates should be installed.

Allow staff and third parties minimal access to IT equipment, systems and information. Access controls should be allocated on the basis of business need. Keep items physically secure to prevent unauthorised access.

Home and mobile working

Develop a policy for home and mobile working and ensure staff are trained to follow it. Devices need to be securely configured with anti-virus software, an updated operating system and encryption. Connection to the business systems and data should be secured, for example, through a Virtual Personal Network service.

Website testing

Websites can be altered fraudulently, and without a firm's knowledge, to include the insertion of false email addresses and phone numbers, leading to clients being lured into providing personal details or paying money into the wrong account. Check your own website regularly or get an outside agency to do so.

Cloud computing and collaboration platforms

Ensure that cloud portal/platform login credentials are secure by following a strong password policy. Enable and configure portal security controls such as IP whitelists and two-factor authentication. Make sure that you and your employees recognise when a cloud-based system is being used and when it might not be appropriate to send or store information via a cloud-based system.

Reduce risk of invoice hijacking

Warn your clients never to send funds to a new account without speaking to the relevant person in the office first; remind clients to check the addresses of any emails purportedly sent by your firm, particularly if they relate to payment of funds. Consider adopting a cybercrime disclaimer warning on your terms of engagement letters and as a footer on all correspondence. This could advise that the firm's bank account details will not change during the course of a transaction; the firm will not change bank details via email; and, clients should check the account details with the firm in person if they are in any doubt.

Notification requirements and incident response

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018
Under GDPR and the Data Protection Act 2018, businesses and their staff are responsible for the security, compliance and governance of their data. GDPR is based around six privacy principles together with the accountability principle. In addition to these principles, individuals have specific rights in relation to their personal information placing certain obligations on organisations that are responsible for processing it. An overview of these principles is available on the Information Commissioner's Office website: **www.ico.org.uk**

Notification requirements
GDPR introduces a duty on all organisations to notify the relevant supervisory authority about certain types of personal data breach. Where a cybersecurity breach is likely to result in a risk of adversely affecting individuals' rights and freedoms, GDPR requires that the data controller notifies the Information Commissioner's Office without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. Where there is high risk to individuals, you must also inform the affected individuals without undue delay. This is not required if appropriate technical and organisational protection measures have been applied to the personal data, such as encryption and, possibly, pseudonymisation. You will also have to notify the police when it is suspected that the breach has arisen from a criminal act. An organisation is considered to be aware when it has a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised. For more information, see the Law Society's *Guide to GDPR*: **www.lawscot.org.uk/gdpr**

If you are a victim of fraud, you must immediately contact your bank, the police and your broker.

Where to get additional help

Cyber Essentials

Cyber Essentials is a UK Government-approved scheme aimed principally at micro-businesses and SMEs. It is required for many UK Government contracts. The Cyber Essentials scheme explains what you need to do and can reassure your clients that you are taking the threats seriously. There are two versions: Cyber Essentials and Cyber Essentials PLUS.

Cyber Essentials

Certification consists of online completion of a self-assessment questionnaire which is then reviewed by a certifying body.

- Certification based on self-assessment/completion of questionnaire.
- Assessment typically costs £300, but additional support is usually required for small firms.

Cyber Essentials PLUS

Certification as for Cyber Essentials, together with system auditing by an independent assessor.

- Assessment typically costs around £1,500, with additional costs to support preparation.

Other resources

Law Society of Scotland
www.lawscot.org.uk/cyber

Cyber Aware
www.cyberaware.gov.uk

Scottish Business Resilience Centre
www.sbrcentre.co.uk

Our thanks

The second edition of our cybersecurity guide was compiled with the kind assistance of Mitigo Cybersecurity
www.mitigogroup.com

The Law Society of Scotland

Atria One
144 Morrison Street
Edinburgh
EH3 8EX
T:+44(0) 131 226 7411
F:+44(0) 131 225 2934

www.lawscot.org.uk