Guide to cybersecurity

In association with
Introduction

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

Year on year, an increasing number of businesses have been affected by frauds and scams, with several high-profile data breaches. A survey commissioned by the UK Government found that 46% of British businesses experienced a cybersecurity breach or attack last year. In 2016, the value of fraud committed in the UK reached £1.1 billion.

Professional service firms, such as law practices, are at particular risk because they hold large amounts of detailed data. Recent figures show that the most severe breaches can cost small to medium-sized businesses more than £300,000.

Solicitors in all fields of practice are increasingly required to know and understand cybersecurity issues – and they are generally well equipped to do so, not least because they understand the principles of the duty of confidentiality, which can be used to encourage more robust data protection to safeguard clients’ interests. Often, firms are at most risk by not following the basics. This guide outlines some of the key threats and risks, 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.
Critical cybersecurity risk areas for solicitors include:

**IT systems**
System security can be compromised in many ways. For instance, cybercriminals can use information leaked over the phone or in hard copy to access IT systems.

**Staff**
Without proper training, staff unaware of risks can disclose data or make unauthorised transactions, particularly where phishing is involved. There is a tendency to share passwords in the workplace due to confidence in colleagues and convenience. Insider threat from unhappy staff is also an issue.

**Sub-contracting**
Sub-contracting, particularly to cloud-based software services creates risk without proper diligence and contracts in place. These providers are generally unwilling to accept much liability.

**Using cloud computing unconsciously**
Many firms have consciously moved to virtual business solutions for their document management and practice management systems. However, many firms are using the cloud unconsciously – anyone using Dropbox, Gmail, Hotmail or mobile apps is almost certainly using the cloud.

**Remote working**
Staff working remotely when travelling or at home are more inclined to make compromises on security by using personal email accounts or insecure connections.

**Personal IT equipment**
Personal IT equipment is increasingly used for work purposes, especially for the mobile workforce. This is more easily attacked than corporate IT resources. Response and disaster recovery – the consequences of a cybersecurity breach can be magnified without a well thought out response and disaster recovery plan.
The threats

The terms cyberattack and cyber-breach are often used interchangeably – but the two are actually quite different.

**CYBERATTACK**

A cyberattack involves someone gaining unauthorised access to a protected computer/IT system. It is caused by people with malicious intent who are cracking into a firm’s systems in ways that cause problems.

**CYBER-BREACH**

A cyber-breach is a broader category, indicating any spill of confidential data, including those that happen by accident and without malicious intent, such as a mistake, negligence, or some other unintentional cause.
The threats
Cyber threats can be categorised as either inadvertent or deliberate.

INADVERTENT THREATS
A lack of knowledge or understanding about basic cybersecurity often leads to data breaches and security weaknesses. The main types of inadvertent threat are:

Human error
Even when acting in good faith, people make mistakes, with errors including poor judgment and failures to follow security procedures.

Out-of-date software
Systems must be updated with the latest software upgrade, known as a patch.

Accidents
Fires, water pipe breaks, physical damage to computer equipment, and accidental deletion of information all pose a threat to IT systems.

Disruption of infrastructural services
Outages of power, water, phone line breakages and similar events could all cause disruption.

DELIBERATE THREATS
Deliberate cyberattacks could be the result of a weakness in technology or because an individual has been manipulated to allow an attack to be instigated. The main types of deliberate threat are:

Malware (malicious software)
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.

Phishing
This type of attack is generally received via spam emails that appear to come from a legitimate organisation, for instance, a bank. 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.

Hacking
An attack by someone trying to remotely access a company 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.

Invoice hijacking
A scam that involves fraudsters intercepting correspondence between two parties who have an existing contractual relationship. The fraudsters then invoice 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 is likely to damage client relations and may cause reputational harm.

Social engineering
Humans are the weakest link in cybersecurity, and attackers use freely available information to pick out who is likely to be vulnerable. For example, the announcement of a planned merger could alert attackers that sensitive bid information may be available to steal. Information from social media, such as Twitter, Facebook and LinkedIn, can be very useful as people often discuss 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.
The threats
Cyber threats can be categorised as either inadvertent or deliberate.

**Trojan**
A type of malware that is usually spread by some form of social engineering. Typically, an end user will browse to a website that prompts the individual to run a Trojan. The websites that carry this out often appear to be legitimate and trusted. Messages are used to persuade the individual to click on a link, for instance, claiming a device is infected with a virus or a computer is running slow.

**Ransomware**
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 is paid to the criminals, who then send the victim instructions on how to unlock the data. This is currently very common due to its ease of implementation and ability to extort funds directly from victims.

**Web seeding techniques (such as malvertising)**
These attempt to exploit vulnerabilities in frequently visited websites. The websites are hacked and used to deliver malicious software through adverts and downloads.

**DDoS (distributed denial of service)**
Attackers exploit the way systems provide services, such as email, information access requests and network timings. 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 to smaller entities.

**Microsoft Office macro infections**
A small program that runs in Microsoft Office applications and is increasingly being used to infect victims’ computers.

**APT (advanced persistent threat)**
An APT attack borrows from other threats, such as phishing and social engineering. The phishing mechanism in this attack is known as spear phishing, which involves sending emails to multiple employees. A Trojan is usually attached in the hope that at least one individual will mistakenly run the malware. Once this is started, the entire network can be quickly compromised. These types of attacks are difficult to identify as they involve detecting unusual patterns of activity on a network.

**Virus**
A type of malware that, when executed, replicates by reproducing itself (copying its own source code) by infecting other computer programs by modifying them.

**Vishing (or voice phishing)**
The victim receives a phone call from someone claiming to be from a bank’s fraud unit. The caller may know the victim’s name and account number. In the case of a firm, the caller will often ask 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 fraudsters 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.
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 operate in a safe and secure environment, and expect high standards. A security breach will cause reputational damage and could result in loss of existing and potential clients.

**Breach of statutory obligations**
The Data Protection Act 1998 requires appropriate technical and organisational security measures to be applied to protect data that individuals can be identified from. If steps have not been taken to prevent a cybersecurity breach, liability for breaching this legislation can result in fines of up to £500,000, enforcement notices, or an investigation from the data protection regulator, the Information Commissioner’s Office. From 25 May 2018, a new data protection law will put in place higher standards to protect security of data and higher fines for breaches.

**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.
Total security can never be guaranteed, but following these basic steps will help to prevent most data breaches and cyberattacks. Cybersecurity is not simply an IT issue – a security culture should be instilled among all staff.

Information security within the office
- Never share passwords – 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.
- Do not leave sensitive information lying around or on the walls – if your desk is a mess, you could accidentally leave sensitive information out and then not notice if it went missing.
- Always lock your computer – make sure you lock your computer when it is unattended to prevent unauthorised access.
- Safe disposal of confidential documents – dispose of paper copies of confidential information securely.
- Encrypt any remote devices that are being sent in the mail – unencrypted USB or other storage devices sent in the mail can get lost or stolen.

Emails
It is easy to become complacent about emails because they are so familiar – but they are not as secure as you might think. In a US court case, Google advised that Gmail users could not rely on their emails remaining private. If you are sending sensitive or confidential information by email, it should be encrypted.

Solutions ~ tips for individuals
Sending emails
When sending emails to external addresses ask yourself:
• Are you allowed to share this information with the addressee?
• Can the information be sent openly or does it need to be protected?
• Has it got a security label?
• Is it personal or confidential information?
• Who is it going to?
• How is it being sent?
• What kind of protection would the email require?

Receiving emails
When receiving emails, think before you click on embedded 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? Be aware, spammers 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 aware 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.
Solutions ~ tips for individuals

Using the telephone
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.

Browsing the internet
• Bogus websites – when browsing the internet, 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 company or a client.

Passwords
Change your passwords regularly and ensure that they are of a certain length. Traditional advice is that an obscure password with a mix of capitals, special characters and numbers is best. 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 lengthy password (eg 40-60 characters).

Working on the move
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. Do not be overheard or overlooked and keep your devices with you at all times.
• 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.
• Leaving public transport – check that you have not left anything behind when you leave, such as your USB stick, documents, laptop or other remote device. Always double check.
• Remove your pass – make sure you remove any security passes before you leave work.

Working from home
• 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.
• Printing – paperwork should be stored and disposed of securely.
• 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.
• Document disposal – do not throw sensitive or confidential documents in the bin. Dispose of paper documents just as securely as you would in the office.
• Mobile phones – when dealing with sensitive information over the phone, be aware who might overhear, purposely or not.
• Keep information discreet – do not leave information lying around for others to see.
• 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. Connect to the firm network using a virtual private network (VPN). If using a wireless network, ensure a minimum of Wi-Fi Protected Access 2 (WPA2) with a good security key.
Risk-based assessments
Make a risk-based assessment of your firm’s information security requirements. Take these 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.
• Ask if others have been affected – consider whether your firm could be a target. Ask around to see whether any of your major clients or any similar firms in your area have been attacked, so you can learn from their experiences.
• Carry out an audit of any assets that are potentially at risk – identify the financial and information assets that are critical to your firm, and the IT services you rely on, such as the ability to take payments via your website. Assess all the IT equipment within your firm, including mobile and personal IT devices. Understand the risks to these by considering how they are currently managed and stored and who has access to them.
• Assess strength of passwords – assess the levels of password protection required to access your equipment and/ or online services by your staff, third parties and clients, and whether it is enough to protect them.
• Policy on data security – you should prepare and issue a clear policy on data use to staff. Appoint a member of staff to oversee the policy, which should include: advice to your employees on the use of business internet facilities for their personal matters; use of social media; and, policies on bring your own device (BYOD).

Education 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.
• Expert advice – decide whether you need to seek expert advice to get the right security controls in place for your firm.

Systems and security controls
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 these 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.

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

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

Secure configuration
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 privileges
Manage appropriately – 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.

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

Smartcard Digital Signatures
For solicitors, encourage the use of digital signatures – there are several issues around both wet and digital signatures, but in many settings a digital signature will offer greater certainty and security. The signature also “locks” the document and prevents any amendment – compared to a paper contract where a page could be carefully removed and replaced, for instance. There is further advice on this on our website.
Encrypt sensitive data
Ensure that sensitive data is encrypted when stored or transmitted online so it can only be accessed by authorised users.

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 and to prevent malware from being installed.

Cloud computing
Cloud computing is in common use. 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 – ensure your firm’s anti-virus software is up to date; 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. More information on how to avoid invoice hijacking is included in the Lockton guidance (locktonlaw.scot). 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 that clients should check the account details with the firm in person if they are in any doubt.
Your systems and procedures should be reviewed regularly

Take these steps to review your security 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 deletion of accounts when they leave.
- Your firm’s website – 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.
- Post-breach review – if your firm is disrupted or attacked, ensure that the response includes 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.

What else can your firm do to ensure maximum protection?

Your firm might want to obtain ISO9001 or ISO27001 compliance (please note these will require significant levels of IT governance). As a minimum, we suggest that you should be getting Cyber Essentials certified.

ISO compliance

- ISO9001 – the internationally recognised standard for quality management systems. Certification to ISO9001 for quality management is commonplace among UK organisations.
- ISO27001 – a specification for an information security management system. There is an increasing requirement for firms to be certified to the ISO27001 standard for information security.

Cyber Essentials

There is an increasing drive from government departments to ensure that commercial companies in their supply chain conform to best cybersecurity practice. Every firm should implement the UK Government’s Cyber Essentials scheme, which sets out the minimum technical security standard that all firms should meet. This will provide you and your clients with reassurance that you are taking the basic steps necessary to mitigate the cyber risk.
The Data Protection Act 1998
All businesses are currently subject to the requirements of the Data Protection Act 1998 (DPA). Under the DPA, businesses and their staff are responsible for the security, compliance and governance of their data. The role of the individual is very important in meeting these requirements. The DPA is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it. An overview of the main provisions of DPA can be found in the Guide to data protection on the Information Commissioner’s Office website.

The General Data Protection Regulations (GDPR)
– European Union legislation
The legislation for this was adopted last year and is expected to be implemented in May 2018. By that time, the UK’s status within the EU may have changed. However, according to the Information Commissioner’s Office (ICO), the regulations will still have an impact on UK firms. This will certainly be the case for any organisations that expect to operate within the EU or to trade within the single market. The requirements under GDPR are broadly similar to DPA but they give additional weight to the rights of the subjects of any data collection, most obviously, in terms of penalties.

If you are already operating good risk management, including being transparent about your data collection and storage and ensuring that your clients consent to you collecting and recording your data, then GDPR is not likely to be very onerous. But it is worth checking the Lockton website, which has useful guidance on GDPR and what it means for you. You should also check the ICO website and the Law Society of Scotland website for updates, because the precise requirements are likely to evolve over the coming months.

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

Notification requirements and incident response
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 sponsors**
- Quorum
  www.qnrl.com
- Sapphire
  www.sapphire.net
- Locktons e-learning
  www.locktonlaw.scot/news/

The guide was produced by a working group of the Society’s Technology Law and Practice Committee. The group was made up of experienced legal technology practitioners as well as academics with expertise in information security and data protection.