IT Security: Keeping information and money safe

26 December 2017

This report highlights the ever growing risk of cybercrime. We all need information technology, so we all need to be aware of the threats.

Download (PDF 20 pages, 441KB) [/globalassets/documents/sra/research/it-security.pdf?version=4a1ad0]

Introduction

We all know that cyber security is an ever growing risk – and cybercrime is now in fact the most prevalent crime in the UK. We all need information technology, so we all need to be aware of the threats.

Cybercriminals are not just after money but are looking for sensitive information too, so the legal services sector is an obvious target. In the last year we have had reports of around £7m of client money being lost to such crime. And I know from my regular conversations with law firms and insurers that this is an area of serious concern for many of you.

It is the job of firms to take steps to protect themselves and their clients, but we want to help. Cybercrime risks evolve rapidly. That is why we provide regular updates on this area - most recently in our July risk outlook. This report builds on that, offering legal professionals a practical, up-to-date guide on how to manage your online security - from cloud computing to the latest cybercrime trends.

Protecting yourself – and your clients - from threats requires constant vigilance. The most commonly reported attack against law firms is email-modification fraud, which not only relies on weaknesses in systems but also on deception. It shows that while antivirus systems are important, well trained and well informed staff are even more so.

We recognise that no defence is perfect, but if you lose client money or information, you need to report these cases to us. We will take a constructive and engaged approach, particularly if you are taking steps to make good any losses to the client, and are looking to learn from the incident. The section in this report on regulatory responsibilities will help you with what you need to do.

After all, there is a bigger picture here. We all need to know what is happening, what the latest cyber attacks are and how we can avoid being caught out. By updating us we can update everyone else. We can all work together to keep the legal sector as safe as possible, protecting firms and protecting your clients.

The facts

- £1 billion was lost to business from online crime (2015-2016)
- £2.3 billion was lost by global businesses from email fraud (2013-2015)
- 75% of cybercrime reports to us are Friday afternoon fraud
- £1.57 million was paid by businesses in ransoms (2016: Q1)
- 43% of all cyber attacks are aimed at small businesses

- 9 security breaches in 2015 featuring more than 10million personal records being exposed

Sources: Action Fraud [http://www.actionfraud.police.uk/news/over-1bn-lost-by-businesses-to-online-crime-in-a-year-jun16] , CRN [http://www.crn.com/slide-shows/security/300081538/10-cybersecurity-lessons-learned-in-2016-so-far.htm/pgno/0/1] , FBI, Symantec [https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16320512&om_ext_cid=biz_email_elq_&elqTrackId=3f9e79f4cbf14b9a9d39e52f9e438f5f&elqaid=2902&elqat=2]

Paul Philip

Chief Executive

Open all [#]

Data protection and cloud computing

Cloud computing

Cloud computing means storing, accessing and processing information on a network of remote servers managed by a third party and accessed over the internet, rather than holding data on a local computer. It is a form of outsourcing.

Cloud computing has been available for many years but it is now more accessible than ever before. It has become the main way in which businesses handle at least some of their data needs. The vast majority of businesses now use cloud computing in some form.

95% of businesses now use cloud computing compared to 30% in 2013

Source: Cloud Tweaks, Rightscale

The advantages of cloud computing include:

- Cost: cloud computing can be much cheaper than maintaining local resources. It can also reduce the need to employ IT support and for new computer equipment, as the processing and maintenance happens elsewhere.
- Flexibility: it is easy to scale cloud computing resources up or down to meet requirements, and contracts can be very flexible. Newer versions of software are also easier to acquire.
- Mobility: accessing cloud resources on the move, anywhere, is as simple as it is from an office desk. A variety of devices can be used to access the same information, with 'virtual desktops' providing the same experience on any device.
- Resilience: with resources in the cloud rather than on a specific device, the risk of data loss from system failure is reduced. It can also help in dealing with some cybercrime threats, such as distributed denial of service (DDoS) attacks1 [#n1] .

This is why so many law firms use cloud computing2 [#n2] . There are, however, associated risks that include:

- Control: as with any outsourcing, cloud computing gives the task of compliance to the remote business while keeping responsibility with the owner. It may be hard for the owner to see whether the outsourcer is acting compliantly or not.
- Compliance: law firms must meet their legal obligations including duties under the Data Protection Act 1998 (DPA) and their regulatory obligations under the SRA Code of Conduct when handling client data. It is important to be sure that their chosen provider can meet these requirements.
- Downtime and data loss: no IT system, whether in the cloud or locally based, is guaranteed to

work all the time. Cases of data loss due to cloud system failures are rare, but have happened[3] [#n3] . Law firms should check their provider's service level agreement, contingency plans and reliability.

- Provider failure: law firms should be sure they know what will happen if their provider becomes insolvent. This is less likely to happen to the largest cloud providers, but any business can fail.
- Changing provider: law firms should be sure of the exit terms in their contract with the provider, including how they retrieve their data.
- Security: the ability to access cloud systems from anywhere means that access controls are very important.

Firms can manage these risks by carrying out due diligence on potential providers, as they would with any other outsourcer. When it comes to data security, some providers may be able to show compliance with international security standards. Examples of these include certification under the Code of Practice for Cloud Service Providers or ISO27001[4] [#n4] .

Solicitors handle extremely sensitive data. Sending it to an outsourcer, such as a cloud provider, does not remove their professional duties to protect confidentiality. As such, it is reasonable for them to expect the highest standards from their IT providers[5] [#n5] .

Outcome 7.10 of the Code of Conduct requires law firms to be sure that outsourcing agreements preserve the firm's ability to meet its obligations and do not alter their obligations to their clients. In addition, we must be able to exercise our regulatory powers in respect of the firm. This means that there needs to be an agreement that allows us to obtain or inspect the information. This does not need to involve a right for us to physically enter the premises of a cloud data provider.

Data protection

It is important to comply with the DPA when handling personal data. Many cloud providers store data internationally. It can be difficult to establish where any particular item of data is being held. This matters because the Eighth Data Protection Principle states that personal data may not be sent out of the European Economic Area (EEA) unless the country it is sent to ensures an adequate level of protection[6] [#n6] . The European Commission maintains a list of countries that it has found to be adequate.

There are exceptions to this where:

- the EU has an agreement with the country to provide adequate protection
- the data controller puts adequate safeguards in place, such as using model contract clauses.

The DPA and the US

The European Commission has not made a finding of adequacy for the US. This means that any data sent from the EEA to the US must be protected with the recommended safeguards. The EU and US have reached an agreement on how to do this, called the Privacy Shield. This is now in force[7] [#n7] .

The Privacy Shield replaces the old Safe Harbour agreement, and allows EU businesses to send data to the US under certain circumstances. Firms may wish to use their own best judgement when choosing providers who use US servers, to be sure that they have the protection of the Privacy Shield.

Changes in the DPA

The introduction of the EU General Data Protection Regulation, due to apply from May 2018 will have an impact on UK data protection rules.

Following British exit from the EU, data protection rules may change again. Our 'Exiting the EU [/risk/risk-resources/exiting-eu/] ' paper provides more information about a range of issues including data protection.

We will give more details about the implications for law firms as the picture becomes clearer.

Cybercrime

"As real life and online become
indistinguishable from each other, cybercrime
has become part of our daily lives."

Symantec8 [#n8]

Cybercrime is a major concern for businesses. Solicitors are no exception. It is one of the most frequent subjects raised with us in our discussions with the profession.

There are many forms of cybercrime. Some cause inconvenience or disruption to business, such as website vandalism or DDoS attacks that force computers offline. More serious crimes, however, involve the loss, or theft of, money or information.

Types of cybercrime

Most cybercrimes involve some element of trickery. While some target information systems directly, more target the person using the system.

Business disruption

Criminals can try to interfere with the operation of a business. They can do this by changing a website, or by seeking to disrupt online activities.

- Hackers can alter websites or force businesses offline through a DDoS attack.
    - DDoS attacks use large numbers of computers and other digital devices to connect to a service multiple times with the aim of overloading it.

The motive or reason for these attacks can vary and include:

- Online activists trying to disrupt the work of individuals, businesses or their representatives for political, social or economic reasons.
- Businesses that wish to harm a competitor. Some criminals advertise DDoS services to organisations9 [#n9] .

These attacks can temporarily interrupt operations. They may be harmful if they occur at a critical time. They rarely involve unauthorised access to sensitive information or money.

Cloud computing systems do have some resilience10 [#n10] . Web and cloud providers may advertise their ability to withstand DDoS attacks. The prospect of these attacks is an issue that businesses should consider when choosing a provider for services particularly if they depend on an online presence.

Email fraud, phishing and vishing

"Email remains the medium of choice for
cybercriminals"

Symantec11 [#n11]

Modifying or falsifying email is a common form of cybercrime. These frauds cost global businesses over £2.2bn from October 2013 to May 201612 [#n12] . Law firms are among the targets.

Falsified email and telephone calls

'Phishing' involves a criminal sending emails that pretend to be from someone else.

- Mass 'spam' emails are the simplest form of this.
- More dangerous forms impersonate someone trusted by the recipient, such as a supplier, a senior staff member or a current client.
- 'Spear-phishing', also known as 'whaling', is a more targeted form aimed at a specific individual and using detailed research to personalise it.

The aim is often to persuade the recipient to give the sender information or money to which the sender is not entitled. These emails are also commonly used as a means of delivering malware, with the program disguised as an attached document or link.

'Vishing' is 'voice phishing'. It is the same as phishing, but using a telephone.

A common example of phishing which has affected solicitors is the 'CEO fraud'. The criminal pretends to be a senior partner or director and tries to get a junior staff member to transfer money.

Modified email

In addition to impersonating someone, criminals sometimes modify emails directly. This requires them to be able to intercept emails between one party and another, usually by hacking into the email system of one of the individuals.

The most common type that solicitors report to us is 'Friday afternoon fraud'. This involves criminals accessing and altering the client's emails to the solicitor or vice versa. The aim is to alter bank details, in order to redirect completion funds to the criminal rather than the client. It does not occur only on Fridays, but that is a time when many completions take place. It also potentially buys the fraudster time over the weekend before the crime is detected.

Bogus firms

Many bogus firms resemble phishing scams in the way they operate. They pose as solicitors in order to gain trust, and some impersonate existing firms. Some will create websites that copy the identity of a genuine firm, or will use copied email headers in their communications. Our paper In the shadows: risks associated with bogus firms [/risk/risk-resources/risks-associated-bogus-firms/] explores this in more detail.

Malware

Malware are harmful computer programs often referred to as 'computer viruses'13 [#n13] . These are controlled by criminals.

The malware that small businesses, including law firms, may encounter is becoming more sophisticated. One reason for this is that several criminal organisations produce 'off-the-shelf' cyber attack kits. These are cheap and advanced. They allow unskilled criminals with limited resources to carry out complex attacks14 [#n14] .

Malware must be installed on a system to affect it. It normally tricks the user into doing this. Users can download malware in various ways including by:

- opening a fake email attachment that may be disguised as a CV or invoice
- connecting an infected device, such as a memory stick or external hard drive15 [#n15]
- visiting a hacked website that can download malware to visitors – a 'drive-by infection'
- encountering an advert on a website that contains hidden code to download malware – 'malvertising'
- having it installed on the system by a hacker or an insider.

Once malware is on a system, it can perform a range of tasks. It can, for example:

- record everything that is typed over a long period, to obtain passwords or financial details
- copy, modify or delete data on the system
- secretly use the system's resources as part of a large, distributed bot-net network to break passwords or coordinate other attacks
- provide a means for hackers to get into the firm's network and other systems.

Ransomware

Ransomware is a very common type of malware. There are many types of ransomware, but they work in similar ways16 [#n16] . Ransomware:

- scrambles any files it can access and demands a ransom for the key to retrieve them
- does not necessarily just encrypt data: some forms steal information or are part of a wider attack
- uses a range of tactics to get people to pay, including a short deadline, a progressive deletion of files, threats to reveal information, or claims to be a means of enforcing a fine.

The cost of these attacks to business is significant. The consequences can include lost files, a significant loss of time and damage to a firm's reputation and client relationships.

Ransomware is very profitable for criminals. The Cryptowall program made its controllers US$325m from its first appearance in early 2014 until October 201517 [#n17] . This has led to an increasing rate of attacks and the development of more advanced types. The amount of ransoms paid has increased strongly since 2015. In the first quarter of 2016 ransomware payments by businesses were £157m.

Paying the ransom usually results in the criminals revealing the means to recovering affected files. However:

- some victims have lost data permanently despite paying18 [#n18]
- in other cases, paying has simply led to higher demands from the criminals19 [#n19]
- there is also no guarantee that information has not been stolen as well as being encrypted.

Paying ransoms involves giving money to criminals. It encourages and funds the development of more ransomware. Solicitors should consider their duties to the public interest and the rule of law when deciding on ethical questions such as this. Where losses are to be covered from insurance, the solicitor's insurer may also have policies concerning ransoms.

Antivirus systems

Antivirus systems will block malware if they can identify it. They will usually do this by matching programs against a list of known malware and against known ways that malware works. They

cannot provide effective protection against malware they do not know how to recognise. Because of this, it is important to keep antivirus systems up to date, and to avoid relying solely on them to prevent malware.

Hacking

Hacking means the exploitation of vulnerabilities in an IT system to gain unauthorised access[20] [#n20] . The Panama papers leak was the result of hackers exploiting flaws in a law firm's email system[21] [#n21] .

Hacking can be as simple as guessing a weak password. Repeated use of a password across different websites can help hackers[22] [#n22] .

More technical hacking relies on finding faults in programs that make it possible for hackers to gain access that they should not have. These can be the result of mistakes in setting up a system, or can be weaknesses in the program itself:

- Computer programs are highly complex, and unrecognised weaknesses can exist.
- When weaknesses are found, a reputable producer will write and distribute patches to repair the problem.
- The release of these patches publicises the vulnerability, making it possible for hackers to work out how to exploit it.
- Systems remain open to attacks until the users have installed the patch.
- Older programs may no longer be patched by their producer.

This is why it is important to use the latest versions of systems, in particular browsers and operating systems, and to keep them up to date.

Trends in cybercrime

Cybercrime is now a very frequent type of crime encountered by individuals, according to the Crime Survey for England and Wales, as shown in figure 1. There were 3.9m cybercrimes against individuals reported to the Crime Survey over the last year: nearly a third of all offences against individuals.

Figure 1: Number of offences against individuals

Source: Crime in England and Wales: year ending March 2016, Office for National Statistics, 2016
[http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2016#new-estimate-of-58-million-csew-fraud-and-computer-misuse-offences]

Businesses

Online crime cost UK business £1bn between April 2015 and March 2016[23] [#n23] . The types of cybercrimes involved are shown in the 2015 Business Victimisation Survey, which records cybercrimes against businesses as shown in figure 2.

Figure 2: Numbers of cybercrimes against businesses (2015)

Source: Crime against businesses: findings from the 2015 Commercial Victimisation Survey, Home Office, 2016 [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/520345/crime-against-businesses-2015-hosb0316.pdf]

These are not necessarily distinct types of crime. Phishing emails are often used to deliver malware, and malware can be used to gain access for hackers.

Overall, cybercrime is increasing, as shown in figure 3.

Figure 3: Trends in the numbers of cybercrimes against businesses (2014 - 2015)

2015 saw large increases in reports of hacking and phishing incidents against businesses. But they reported fewer cases of malware. The rise in ransomware may change that trend.

Solicitors and regulated firms

The Information Commissioner's Office (ICO) regards solicitors as facing the same types of threats as other businesses. Their figures from the first quarter of 2016 show the legal and justice sectors reporting the fourth highest number of data security cases24 [#n24] .

In respect of the reports being made to us, the vast majority relate to Friday afternoon Fraud. We are aware of losses in the region of £7m in the last year. We do however suspect significant underreporting in this area. We discuss when to report cybercrime to us later in this report.

Figure 4: Reports to SRA of cybercrimes Nov 15 - Jul 16

Motives for cybercrime

Criminals mostly attack law firms for profit. They aim to steal money directly, or steal information that they can use to make money. Research shows that most cybercriminals seek targets that offer a swift, large return25 [#n25] .

Sensitive client information can also be a target for theft. Criminals may see law firms as a 'weak link' compared to the client's own defences26 [#n26] . Even if a law firm does not hold the sensitive information itself, hackers may try to get malware onto the firm's systems as a means of getting it onto the client's systems.

There are many reasons why cybercriminals might steal information. Some examples include:

- identity thieves might be looking for the personal details of clients and their payment information
- a competitor of one of the law firm's clients might be looking for trade secrets or for information about the client's strategy
- state-sponsored hackers might be looking for economic or technology intelligence27 [#n27]
- insider traders can benefit from price-sensitive information
- sensitive information might be used for blackmail.

The consequences of cybercrime

Impact on consumers

Cybercrime can involve the theft of very large sums of money. Cases of 'Friday afternoon fraud', targeting conveyancing proceeds, can lead to losses in the hundreds of thousands. This can be highly distressing and, where it was the solicitor who sent the proceeds to the falsified account, risks the trust placed in solicitors to act in their clients' interests.

The loss of confidential information can also be very distressing and can have emotional and economic impacts. Solicitors have a duty of confidentiality toward their clients and often hold very sensitive information.

Impact on solicitors and law firms

Losses of client information or money affect the solicitor and law firm as well as the client.

Protecting against cybercrime is not easy. It is not possible to avoid all information risks even by avoiding all IT, since physical documents have risks too. One of the options available to manage these types of risks is to insure. Although this should be only part of a wider risk management approach including steps to avoid this risk materialising.

The minimum terms and conditions for solicitors' professional indemnity insurance (PII) may cover losses of client money from cybercrime, limited to the amount actually insured. For some firms dealing in large sums of client money, the minimum cover of £2m for sole practitioners and partnerships and £3m for others such as limited companies, may not always be sufficient. Firms may also wish to consider whether they need cover for their own potential losses from cybercrime, beyond those affecting the client. In the wider business context, it has been increasingly common to take up specific cyber insurance28 [#n28] .

Solicitors using indemnity or additional insurance to manage the risk of cybercrime losses will need to know and comply with their insurers' policies and requirements.

We have recently published information on current trends in PII, based on analysis of ten years of claims data from 2004–201429 [#n29] . This demonstrated that, excluding claims for which the insurer did not categorise the reason, conveyancing was responsible for more than half the value of all insurance claims. Friday afternoon fraud against conveyancing is also the most common type of cybercrime reported to us.

Our publication of the insurance analysis is part of our ongoing development of proposals for changes to the minimum PII cover requirements. We are reviewing whether our rules are encouraging the right behaviours for firms to adopt a wider risk management approach to cybercrime attacks. We will be talking to firms and insurers further to obtain views on this ahead of a formal consultation.

Law enforcement successes

There are international efforts to shut down cybercrime organisations. Some ransomware control systems have been captured and decryption keys seized. Major cybercriminals have been arrested30 [#n30] . However, the international nature of cybercrime makes enforcement challenging.

The No More Ransoms initiative

No More Ransoms [https://www.nomoreransom.org/] is a site dedicated to stopping ransomware. It is a joint initiative between Europol, the Dutch police and IT companies Intel and Kaspersky. It provides a way to recover files affected by four different 'families' of ransomware.

At the time of writing, the site contains 160,000 individual decryption keys, captured from ransomware controllers. This enables victims to recover data without paying if the key for their system is on the site. The site also provides tools to scan systems for ransomware, guidance on dealing with the threat, and a portal to allow victims to report cases directly to their own country's police.

Case studies

The Panama papers

In 2016, 11.5 million documents relating to the activities of offshore shell companies were leaked31 [#n31] . This was the result of illicit access to the systems of Panamanian law firm Mossack Fonseca and was the largest data breach in history. The firm's founding partner believes that the cause was a penetration of the firm's email server.

The email server in question had not been updated since 2013 and contained multiple weaknesses. In particular, the client portal was vulnerable to a well-known attack allowing hackers to type code into a query field on a website, for instance the "name" field on a contact form, and have the website run it to give them control[32] [#n32] . Although the full details of the attack are not known, updating the server to fix these vulnerabilities would at least have made it harder for the attackers to obtain information.

Commercial espionage by a competitor against a small business

In 2015, a commercial laundry service with 35 employees found malware in their computer system. The malware had been stealing customer and price information. On investigation it turned out to have been there for two years.

The attack was traced to a competitor, who had been spying on the laundry service for commercial advantage. The rival business was convicted and was fined US$12K in March 2016[33] [#n33] .

The low cost of off-the-shelf hacking toolkits means that even small businesses like these can carry out, or be the victims of, commercial espionage[34] [#n34] .

Ransomware

In 2016, a hospital found ransomware on its systems. The malware scrambled files related to finances, patient records and medical device instructions. It demanded a ransom for the key to recover the documents, and provided payment instructions.

The hospital decided to pay the ransom. The criminals did not, however, provide information on how to recover files. Instead, they sent further demands for larger payments[35] [#n35] .

Paying the criminals behind ransomware does not guarantee that files can be retrieved. Keeping secure and multiple backups of data is the best defence against these attacks.

Regulatory responsibilities

Your obligations

Solicitors are obliged under the Code of Conduct to maintain effective systems and controls to mitigate risks to client confidentiality[36] [#n36] , client money[37] [#n37] , and to overall compliance with our regulatory arrangements[38] [#n38] . As such, there may also be legal and regulatory consequences for the solicitor or law firm after a breach of confidentiality or loss of client money.

Being hacked, or falling victim to malware, is not in itself a crime or necessarily a failure to meet our regulatory requirements. No defence is perfect. But we do expect firms to take proportionate steps to protect themselves and their clients' money and information from cybercrime attacks while retaining the advantages of advanced IT.

If a law firm loses client money or information to cybercrime we will consider whether there has been a breach of our Code of Conduct. Firms should report these cases to us even where, in the case of stolen money, that money has been replaced.

Outcome 10.3 says:

you notify the SRA promptly of any material changes to relevant information about you including serious financial difficulty, action taken against you by another regulator and serious failure to comply with or achieve the Principles, rules, outcomes and other requirements of the Handbook.

We will judge whether it is appropriate to take any action on a case by case basis according to the facts of the incident. We will take into account whether the firm had adopted reasonable systems and controls to protect against the risk.

When we do receive a report about cybercrime, we will aim to take a constructive approach in dealing with the firm. This will particularly be the case if the firm:

- is proactive and lets us know immediately
- has taken steps to inform the client and as a minimum make good any loss
- shows they are taking steps to improve their systems and processes to reduce the risk of a similar incident happening again.

It should also be noted that solicitors and law firms, like any business, can be reported to the Information Commissioners Office (ICO) for breaching the Data Protection Act (DPA)39 [#n39] .

Letting us know about failed attacks

We are in a better position to advise firms on how to protect themselves if we learn about failed incidents as well as about successful attacks. It is also helpful if we learn about cases where the client has been affected by cybercrime without the solicitor being involved. An example would be where the client has been tricked into sending money to criminals rather than to the solicitor.

This information lets us know about the trends in cybercrimes against law firms and helps us produce scam alerts and warnings to help prevent others falling victim to attacks40 [#n40] .

Steps you can take

When setting out to secure your systems, a reasonable aim is to become a harder target for criminals. A good defence – including well trained staff – will deter most attackers.

Business culture

In deciding how to protect yourself, it is useful to start by looking in the broadest sense at your firm's control environment – that is to say, your business culture, and your organisational procedures, policies and structures. Many improvements that make the organisation work more efficiently and effectively will also help secure the business against cybercrime.

For example, having efficient processes across the firm for handling money, with clear duties and reporting lines, will help the firm's performance while also improving the service for clients. It may also minimise the amount of money held by the firm at any given time, making the firm a less desirable target for thieves.

There are many specific steps that can also help in protecting you from cybercrime. These do not need to be expensive. When it comes to the technical aspects of configuring computer systems, however, you may find it useful to obtain professional advice.

Detecting Friday afternoon fraud

The great majority of cybercrimes reported to us are forms of Friday afternoon fraud or similar email modification scams. It is worth specifically considering how to address them. Conveyancers and others who hold large sums of client money are at the most risk.

Even for those who do not hold large amounts of client money, it is worth considering this risk. Many supplier frauds and phishing efforts also seek to redirect funds. Systems that help against Friday afternoon fraud will also work against these scams.

Examples include:

- confirm client and third party payment details, for example sending £1 to the account details provided and confirming it has been received
- provide information to clients confirming they will never be asked by you to send money to a different account than that given
- be suspicious of requests to change payment details, in particular those sent by email with high urgency, and confirm them with the client on a known telephone number
- consider using a lawyer checker service to confirm that money sent to details provided by a third party lawyer is genuinely going to them.

Business policies and systems

It is important to maintain policies and procedures that protect information security.

Examples include:

- make sure only approved staff can transfer money
- take advice from your insurer on any steps that they require or recommend
- consider certification schemes such as Cyber Essentials [https://www.gov.uk/government/publications/cyber-essentials-scheme-overview]
- handle client money efficiently, for example, using fixed fees to avoid the need for money on account, taking deposits as late as practicable
- regularly audit your data systems and sample files
- review your protection arrangements to ensure that they are kept up to date.

Training

Most cybercrimes target people rather than systems, for example using phishing. The best defence is to learn, and to train your staff, to:

- recognise common scams, such as Friday afternoon or CEO fraud
- avoid opening unsolicited email attachments
- avoid connecting unapproved devices, such as personal memory sticks, to firm systems
- use good passwords, change them regularly and use more secure authentication systems where available
- do not open electronic information in a place where members of the public can view your password or the documentation being opened
- adopt a robust process to confirm any requests to change payment details
- keep track of your online presence to spot bogus firms copying your identity
- monitor social media posts to make sure they do not contain information that could be of use to criminals.

IT systems

It is important to secure your IT system to keep out malware and hackers. Many serious data leaks have happened because a firm did not take basic measures. Cost-effective steps that you can take include:

- keep software, including but not limited to operating systems and internet browsers, up to date
- only install trusted software onto your systems
- use an antivirus system and keep it up to date – but do not rely only on this to keep malware out
- use encryption on mobile devices, and consider encrypting documents more generally
- back up your files on a regular basis ideally including at least one 'cold' backup – one that is not directly and regularly connected to your main systems
- take professional advice about any issue you are not sure of when setting up your system
- set up access controls so that, as far as possible, staff can only access and alter certain files, and restrict the ability of employees to install software
- avoid distributing files by email attachments or flash drives/memory sticks
- set up secure remote access to avoid the need for staff to carry files or to store data on mobile devices, if they work in transit or remotely
- consider software to block online advertising, and restrict the ability of web browsers to run common vulnerabilities such as Javascript or Flash programs, as all these can be means of distributing malware
- consider adopting digital signatures and encrypted email to verify identities and help prevent interception of communications.

If you believe you have been the victim of cybercrime

Sometimes, cybercriminals manage to steal money or data. If there has been a cybercrime attack resulting in loss of client money or data you should:

- report the incidents to us [/home/contact-us/]
- notify Actionfraud [http://www.actionfraud.police.uk/]
- be aware of when you need to notify your insurers or the ICO
- take professional IT advice on how to remove any malware41 [#n41]
- review the incident and fix any security holes, as businesses who have had one cyber attack succeed can expect repeated attacks within the same year42 [#n42] .

Where to go for further information

Cloud computing and data protection

The ICO [https://ico.org.uk/for-organisations/] provides advice and self-assessment tools on its website. This includes specific guidance on the use of cloud computing [https://ico.org.uk/media/1540/cloud_computing_guidance_for_organisations.pdf] and for small businesses who want to outsource data internationally [https://ico.org.uk/media/1585/outsourcing_guide_for_smes.pdf] . This would cover the use of cloud computing providers who store data overseas.

Cybersecurity

Cyber Essentials [https://www.gov.uk/government/publications/cyber-essentials-scheme-overview] is a government-backed scheme offering proportionate guidance for all sizes of business on how to deal with information security risks.

Action Fraud [https://www.actionfraud.police.uk/] is the UK national reporting centre for fraud and cybercrime. It is part of the City of London Police, which is the national lead on fraud. In addition to guidance, they provide an online fraud reporting tool for those who have been affected.

If your systems are affected by ransomware, check whether the No More Ransoms [https://www.europol.europa.eu/content/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-fight-ransomware] initiative has the decryption keys for that type. The same site gives advice on how to prevent and report ransomware attacks.

For any malware attack, your antivirus provider may have information about how to remove the program once you have found it on your systems, and about how to recover.

We produce regular up to date information about cybercrime and other issues on the Priority Risks [/risk/risk-outlook/] page of our website.

Notes

1. DDoS attacks use a large network of computers to make access requests to a system, overloading it and forcing it offline.
2. See for example Why move to the cloud?, Salesforce, 2015 [https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html]
3. What happens when data gets lost from the cloud, Cloud Computing News, 2015
4. Code of practice for cloud service providers, Cloud Industry Forum, 2016; International standard for information security management systems (ISO/IEC 27001 2013), ISO/IEC, 2013 [https://www.cloudindustryforum.org/content/code-practice-cloud-service-providers]
5. Improving regulation: proportionate and targeted measures, SRA, 2015 [/sra/consultations/consultation-listing/regulatory-reform-programme/]
6. Sending personal data outside the European Economic Area (Principle 8), Information Commissioner's Office, 2016
7. EU-EU Privacy Shield, European Commission, 2016
8. Internet security threat report 2016, Symantec, 2016 [https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16320512&om_ext_cid=biz_email_elq_&elqTrackId=3f9e79f4cbf14b9a9d39e52f9e438f5f&elqaid=2902&elqat=2]
9. Gwapo's professional DDoS service, Daily Motion, 2014 [http://www.dailymotion.com/video/x2558pm_gwapo-s-professinal-ddos-service_news]
10. DDoS, the cloud and you, The Register, 2016 [http://www.theregister.co.uk/2016/07/21/ddos_the_cloud_and_you/]
11. Internet security threat report 2016, Symantec, 2016 [https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf]
12. Business email compromise: the 3.1 billion dollar scam, FBI, 2016
13. Technically, a virus is one specific type of malware, capable of distributing itself to other systems. Most malware actually in use is of the 'trojan horse' type, installed by deception on just one system without the ability to infect others. In practice, these terms are used interchangeably.
14. Exploit kits as a service: how automation is changing the face of

cybercrime, Heimdal Security, 2016 [https://heimdalsecurity.com/blog/exploit-kits-service-automation-changing-face-cyber-crime/]

15. The infection could be intentional or accidental. Leaving an infected memory stick in the carpark of the target business, for staff to pick it up and connect it, has been a repeated and successful tactic used for both cybercrime and espionage purposes.
16. Ransomware 101: what, how and why, Trend Micro, 2016 [http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works]
17. Cryptowall ransomware raised $325m, IT Pro, 2015 [http://www.itpro.co.uk/security/25515/cryptowall-ransomware-raised-325m]
18. Posing as ransomware, Windows malware just deletes victims' files, Ars Technica, 2016 [http://arstechnica.com/security/2016/07/posing-as-ransomware-windows-malware-just-deletes-victims-files/]
19. Kansas Heart Hospital hit with ransomware: attackers demand two more ransoms, Network World, 2016 [http://www.networkworld.com/article/3073495/security/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html]
20. Some sources use 'cracking' to refer to the use of hacking for criminal purposes, and reserve 'hacking' for benign activities such as penetration testing.
21. Why cybercriminals are targeting law firms, D Magazine, 2016
22. Sharing your password, Indiana University, 2016
23. Over £1bn lost by businesses to online crime in a year, Action Fraud, 2016 [http://www.actionfraud.police.uk/news/over-1bn-lost-by-businesses-to-online-crime-in-a-year-jun16]
24. Data security incident trends, Information Commissioner's Office, 2016 [https://ico.org.uk/action-weve-taken/data-security-incident-trends/]
25. Flipping the economics of attacks, Ponemon Institute, 2016 [https://www.paloaltonetworks.com/content/dam/creative-assets/campaigns/corporate/ponemon-report/web-assets/PAN_Ponemon_Report.pdf]
26. Corporate espionage: the reason law firms are a big hacking target, Lexblog, 2015
27. State sponsored cybercrime: a growing business threat, Dark Reading, 2015 [http://www.darkreading.com/vulnerabilities---threats/state-sponsored-cybercrime-a-growing-business-threat/a/d-id/1320555]
28. Benchmarking trends: as cyber concerns broaden, insurance purchases rise, Marsh Risk Management Research, 2015 [http://www.oliverwyman.com/content/dam/marsh/Documents/PDF/US-en/Benchmarking Trends Cyber Concerns Broaden, Insurance Purchases Rise-03-2015.pdf]
29. SRA publishes data ahead of insurance consultation, SRA, 2016 [/sra/news/press/2016/pii-trends-published/]
30. Interpol arrests business email compromise scam mastermind, Trend Micro, 2016 [http://blog.trendmicro.com/trendlabs-security-intelligence/interpol-arrests-business-email-compromise-scam-mastermind/?_ga=1.45483300.1868705472.1473254602]

31. Why cybercriminals are targeting law firms, D Magazine, 2016
32. Known as ‘SQL injection’: see The security flaws at the heart of the Panama Papers, Wired, 2016 [http://www.wired.co.uk/article/panama-papers-mossack-fonseca-website-security-problems]
33. New Hampshire company pleads guilty to hacking into a competitor’s computer system for commercial advantage, FBI, 2015 [https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/new-hampshire-company-pleads-guilty-to-hacking-into-a-competitors-computer-system-for-commercial-advantage]
34. New Hampshire company pleads guilty to hacking into a competitor’s computer system for commercial advantage, FBI, 2015 [https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/new-hampshire-company-pleads-guilty-to-hacking-into-a-competitors-computer-system-for-commercial-advantage]
35. Kansas Heart Hospital hit with ransomware: attackers demand two more ransoms, Network World, 20165 [http://www.networkworld.com/article/3073495/security/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html]
36. Outcome 4(5), SRA Code of Conduct 2011 [/solicitors/handbook/code/]
37. Outcome 7(4) SRA Code of Conduct 2011 [/solicitors/handbook/code/part3/content]
38. Outcome 7(2) SRA Code of Conduct 2011 [/solicitors/handbook/code/part3/content]
39. Guidance on the use of monetary penalties, Information Commissioner’s Office, 2016 [https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf]
40. Flipping the economics of attacks, Ponemon Institute, 2016 [https://www.paloaltonetworks.com/content/dam/creative-assets/campaigns/corporate/ponemon-report/web-assets/PAN_Ponemon_Report.pdf]
41. Basic advice is available from many antivirus vendors, and detailed post-incident response assistance may be available through your insurer or IT services provider in some circumstances.
42. Internet security threat report 2016, Symantec, 2016 [https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16320512&om_ext_cid=biz_email_elq_&elqTrackId=3f9e79f4cbf14b9a9d39e52f9e438f5f&elqaid=2902&elqat=2]