Solicitors Regulation Authority

How to reduce the risk of being affected by cybercrime

23 November 2020

Introduction

As our reliance on advances in technology in the legal sector increases, so too does the risk that firms will be exposed to cybercrime. Firms provide a convenient doorway for fraudsters to access confidential information and client money and increasing numbers have been the focus of targeted cyberattacks.

We received 458 reports of cybercrime incidents between 2016 and 2019, but we suspect that this may not represent the true total of attacks experienced by firms. We visited 40 firms who made a report to find out more about these incidents. You can read detailed analysis about the findings in our thematic review [https://consultations.sra.org.uk/sra/how-we-work/archive/reports/cyber-security/] .

Who is this for?

This is a practical resource to complement our thematic report and support those of you improving your cyber security. It highlights the experiences of firms who were targeted by cyberattacks to help you understand the potential impact of an attack and the steps you can take to mitigate similar threats.

We found evidence of good practice at many firms, but also some areas for improvement and both have been included in this report. This will help you to evaluate your firm's approach to cybersecurity and identify if there any gaps in your knowledge or procedures.

However, there is no such thing as a one-size-fits-all model when managing cyber-risks. Your primary focus should be on understanding the specific threats facing your firm and tailoring your response accordingly as these risks evolve. The onus is on you to assess the right steps to protect your firm and your clients, and to take those steps accordingly.

Cyber threats and controls

Our toolkit provides some 'take away' top tips we identified from the firms we visited and focuses on the three most common types of cyber threat they experienced:

- Email modification fraud

- Phishing, vishing and spear phishing
- Malware

The toolkit also examines four key controls that we found can help firms to manage cyber security risks:

- People and training
- Policies and procedures
- Technology
- Managing risks

Use our checklists at the end of each section to check how your approach to cybersecurity and knowledge matches up. Not every point will apply to your firm. Finally, refer to our glossary of common terms in cyber security at the end of this report to enhance your knowledge of this area if required.

Top tips

- Plan your response with a cyber-risk incident plan
- Foster a positive "no-blame" culture
- Monitor, record, analyse and respond
- Integrate cybersecurity into all your processes
- Know your reporting requirements
- Train staff and raise awareness in clients

Cyber threats

Open all [#]

Email modification fraud

Email modification fraud was the most common type of cyberattack experienced by the firms we visited, and most reports concerned clients sending funds to a fraudster’s account. It is also the most common type of cyber incident reported to the SRA, accounting for 68 percent of all reports we receive. Attacks can be very sophisticated, involving almost imperceptible changes to email addresses, for example, in one firm's case, changing an 'O' to a '0' (zero) in their name, while others are more crude attempts. In all cases, time and personal pressures can mean firms and clients miss the signs of an attack.

Some of the attacks experienced by firms were random attacks while others were more targeted with fraudsters monitoring and intercepting emails for example by using email forwarders during a transaction. Modified emails often impersonated the firm or the client in order to obtain money or sensitive information, for example passwords.

Conveyancing transactions were the most common but not the only target in these scams.

Fraudsters also targeted negligence claims, litigation and probate matters but in nearly all cases, they changed the bank account details of one of the parties without their knowledge during the transaction. This resulted in settlements, completion funds and deposits being transferred to the fraudster's bank account.

Case Study: Email modification fraud in a conveyancing transaction

The firm were instructed to act in a property sale. On the day of exchange, the firm received a modified e-mail purporting to be from the client, changing the real client's instructions. The fraudster asked for half of the completion funds to be transferred to another account at the same bank used by the client.

The firm's policy said that staff should seek verbal confirmation of any changes to bank details given by email and they called the client. However, the client was busy and didn't have their details to hand. They instructed the firm to "get on with it". The employee was flustered and despite never receiving confirmation of the account actioned the payment sending the funds straight to the fraudster.

Outcome

The firm contacted the bank, but a significant amount of time had passed, and the funds had been withdrawn, leaving a shortage of £400,000. The firm repaid the shortage immediately but had to take it from the office account, significantly impacting their cashflow.

Although insurers ultimately repaid the firm, they lost their £5,000 excess. Additionally, the client, who was very distressed about the incident, complained to the Legal Ombudsman and the firm were required to pay them £900 compensation.

The firm have now strengthened their policy and insist on written authorisation from the client before they accept any instructions to change bank account details.

Diagnostic Check Up

The SRA Account Rules requires firms to immediately pay into the account or replace any money that has been improperly withdrawn from the client account. Firms should also report this loss to the SRA . We have warned that client money is at risk[2 [#n2]] if your firm is subject to a cyberattack and email modification fraud is a common method of diverting client funds to fraudsters.

Even small firms hold high volumes of funds in their accounts and are an increasingly attractive targets for fraudsters The introduction of the Confirmation of Payee [https://www.wearepay.uk/confirmation-of-payee/] (COP) system by Pay.UK[3] [#n3] this year will provide further protection from bank mandate and email modification fraud, but firms still need to remain vigilant. You also have the option to consider whether a third-party-managed account (TPMA)[4] [#n4] is appropriate for your firm.

Q: Do you have suitable controls to protect client money?

Carry out a health assessment of your firm's controls to manage client money. Are you equipped to protect clients from the impact of email modification fraud? Consider how robust your controls and policies to manage this risk. For example, when changes to banking instructions occur, do you have strategies in place such as requiring a password, identification, or a verbal or written confirmation before transferring funds?

Having adequate safeguards to verify the identity of email senders and raising awareness amongst staff and clients are also key defences against this type of fraud. For example:

- Train staff to regularly scrutinise emails; verify the identity of a sender by hovering your mouse over an email address, check for any variations to addresses or format changes to official logos and note any unusual spelling or grammatical errors.
- Tell your clients that you would never change your bank details by email.

Checklist:

Now, check your answers to the following questions:

- Do you warn clients that you would never change your bank details by email?
- Have you checked whether your email account has been compromised with forwarder rules?
- Do all your communications with clients educate them about the risks of cyber fraud?
- Do your staff feel confident about querying and checking payment transfer requests that feel pressured?
- Are your staff vigilant about spotting the signs of a potentially fraudulent email?

Phishing, vishing and spear phishing

Phishing and vishing were also common cyberattacks at the firms we visited. Fraudsters send emails or make telephone calls to trick the recipient into sending them confidential information or money. Twenty six

percent of the phishing attacks we reviewed were targeted at the client's email account, rather than the firm's account.

Firms reported receiving many unsuccessful untargeted phishing emails but, in most cases, successful attacks appeared to be a targeted (spear phishing) attempt. They often involved a series of communications during which time, trust was established, and information was gathered. This led to the payoff when the recipient's bank account details were changed to the fraudster's bank account.

Some firms told us that they suspected that specific individuals had been targeted because of their role at the firm or a client had been targeted because there had been a supply chain compromise by a third party involved in the transaction.

One of our firms also reported that their accounts department had been targeted by 'CEO fraud,' also known as 'whaling'. A fraudster created a spoof email impersonating a senior member of staff at the firm and successfully persuaded a more junior employee to transfer £8,000 to their account.

Case Study: A successful vishing attack

The firm's accounts department received a telephone call from someone claiming to be an official from the payment security centre team of a well-known bank.

The purported bank official explained that they were concerned that a payment from the firm wasn't going through. They provided an alternative account for them to retry the payment again.

The accounts department complied with the request and made the payment again. However, the bank official told them that unfortunately this payment hadn't worked either and could they try making the payment again, which they did. The fraudster then repeated this again and again until several payments had been made by the firm over the course of an hour.

The firm's employee eventually became suspicious and phoned the bank immediately. However, by that time £1.2 million had been transferred to the fraudster.

Diagnostic check-up: Phishing and vishing

Most of the cyberattacks we saw at firms targeted users' vulnerabilities rather than technological vulnerabilities. Human error is a key risk for firms, and this was particularly the case with phishing and vishing attacks which usually rely on a lack of attention to detail. Phishing and Vishing attacks can seem almost a commonplace occurrence in many

businesses but the consequences for not managing this risk can be severe[5 [#n5]].

Adapting your business culture to prioritise this risk, educating clients, delivering regular training to all staff from senior managers to receptionists and supporting others to report concerns, can help to protect your firm and your clients.

There are also specialised technological options that can help to support your overall cyber security strategy against phishing attacks. For example, DMARC[6 [#n6]]' is recommended by the National Cyber Security Centre (NCSC) as a secure way of configuring email accounts to prevent email modification and protect against phishing email attacks.

Q: How effective are your defences against phishing attacks?

Carry out an assessment of your systems, controls and working practices to check how effectively you manage data with third parties. Test your vulnerabilities with an audit of your systems and processes to check how quickly you can respond to any reported incidents. Consider how useful your data management is, how well you process personal data and how confidential information is secured?

Law firms hold sensitive data and client money. The General Data Protection Regulation 2018 (UK GDPR) requires firms to have appropriate measures in place and take 'appropriate' action to manage these risks [https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/] . Fraudsters can use a weakness in the chain to intercept information and target individual clients or the firm.

Finally, remember that empowered and knowledgeable staff will be your first line of defence to phishing and vishing attacks.

Checklist:

Now, check your answers to the following questions:

- Do you advise clients to be cautious about emails from the firm that seem unusual, have poor spelling or grammar?
- Does your IT system have an effective phishing filter?
- Do you know what 'smishing' and 'spear phishing' is?
- Have you refined your spam filter to make it relevant for your firm?
- Have you considered what information available on your website could be used by fraudsters and whether this can be minimised to mitigate potential fraud?
- Are you aware of 'DMARC [https://dmarc.org/] ' and/or explored monitoring your email system?
- Does your Management Board use a firm wide risk register to focus your response to different cyber risks?

Ransomware

Ransomware is a form of malware or virus which infiltrates a user's computer and holds their data hostage until a ransom is paid. Four firms we saw were subject to a ransomware attack, and all appeared to be opportunistic rather than targeted, usually downloaded as a result of employees clicking on links in phishing emails. Firms were affected to various degrees. Some firms lost access to their entire system, while others lost a limited range of data, for example historical files. There were no client losses but the disruptive effects in some cases were extensive.

None of the firms we met paid a ransom demand. They reported the incidents to the SRA, and all were eventually able to recover their systems. This is a good approach as there are no guarantees that data will be released after a ransom is paid and this may lead to further demands from hackers. You may also be breaching the UK GDPR [https://www.ncsc.gov.uk/information/GDPR] in certain circumstances if you do not recover the data or report the incident.

Case Study: Ransomware attack against a large firm

A fee earner clicked on an attachment in a phishing email containing malicious software over the weekend. The firm discovered they had been subject to a ransomware attack when staff tried unsuccessfully to log on to systems the next day. The malware bypassed the firm’s firewall and encrypted their operating systems, making them inaccessible.

The ransom request was for a payment in the region of $500 and was likely to have been opportunistic rather than a targeted attack. The firm did not communicate further with the hacker or offer to pay the ransom as this was likely to encourage further demands. Ironically, they could not have paid anything even if they had wanted to because the virus had been so successful in locking down their systems.

Outcome

The firm tried to isolate what was left of their system but lost nearly everything stored on their main servers, including file stores and practice management systems. The firm had to shut down while work was carried out to restore the data.

Overall, revenue losses were calculated to be around £150K. However, the biggest impact was the emotional toll on key staff who were working nearly 20-hour days. This stressful experience was highlighted by staff who recalled that the sound of the firm’s emergency group call notification left them with a feeling of anxiety with every call.

Diagnostic Check Up

We expect firms to identify, monitor and manage risks to their business[7 [#n7]] but we understand mistakes can happen and that this can have an emotional impact on staff. Supporting staff by embedding a positive cyber security culture and a transparent, firm wide cyber security strategy can help you manage these risks.

A well-rehearsed disaster recovery plan which sets out contingencies, roles and responsibilities, reporting lines and contact details can also help you to mitigate the risk of ransomware.

However, only 27 firms in our sample had a disaster recovery or contingency plan in place and concerningly, 15 of these firms stored their plans on their systems. This could potentially be a risk if these firms were unable to access their systems in a ransomware attack.

However, only 27 firms in our sample had a disaster recovery or contingency plan in place and concerningly, 15 of these firms stored their plans on their systems. This could potentially be a risk if these firms were unable to access their systems in a ransomware attack.

Q: Could your firm recover easily from a ransomware attack?

Carry out a health check of your contingencies as well as your controls. Review and test them to see how effectively your firm could protect itself from a ransomware attack. A risk-assessment will enable you to determine what your current vulnerabilities are and how damaging a cyber threat could be to your firm.

Consider how prepared you are to respond to a catastrophic loss of data and how quickly you would be able recover and resume your business after disruption. Remember that firms should report any personal data breaches caused by a cyber security incident to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach[8 [#n8]].

Checklist:

Now, check your answers to the following questions:

- Do you warn staff to avoid opening unsolicited emails with links and attachments?
- Do you have an up to date disaster recovery plan?
- Have you compiled an asset inventory of all your software, systems and devices?
- Have you prepared a risk assessment of vulnerabilities and threats and put in place strategies to protect your systems and network?
- Have you updated your risk assessment to reflect changes in your working practices, for instance increased remote working due to Covid-19?

- Is your inventory and contingency plan accessible in the event of a systems failure?
- Do you have enough servers, backups and storage facilities to recover data quickly and are they kept securely?
- Do you keep up to date with the NCSC's guidance materials on ransomware attacks?
- Do you know how malware is most likely to be downloaded on your systems?

Controls

Open all [#]

People and training

No cyber defence is infallible, and as technology advances, so does cybercrime. Its evolution has made cyber threats more sophisticated and difficult to identify and it’s not difficult to see why successful cyberattacks occur.

This can have a personal impact on staff who may be worried about their jobs, overwhelmed by the impact of an attack or their responsibility for an attack. We were concerned that two of the firms we saw reported that they had dismissed employees who had been the target of cyberattacks, and one employee left their firm shortly after being subjected to an attack.

A supportive cyber-aware business culture is more likely to encourage staff to highlight risks to firms. Training and motivating staff to report suspicious emails and manage security challenges when under pressure will help your firm learn from mistakes.

Case Study: People and training

A large firm told us that they had invested heavily in face to face training after experiencing a serious cyberattack. They felt that the most important aspect of managing cyber risks is ensuring that staff are well trained and implementing an engaging and effective training strategy was a key part of this.

They introduced a specific face to face cybersecurity training course because this emphasised to their staff how seriously they considered the risk. They believed that staff were also more likely to be engaged and focus on the material if it was delivered in person surrounded by other team members and senior partners. They subsequently followed this up with refresher training such as online courses.

Their advice to other firms was that you should not wait to have an event before implementing safeguards. ‘Be proactive. It’s when - not if, it

happens!’

Diagnostic check-up: People and training

We expect firms to make sure that managers and employees are competent to carry out their role, and keep their professional knowledge and skills, and their legal, ethical and regulatory obligations, up to date[9 [#n9]]. We were concerned that a small minority of firms had a poor level of knowledge of cyberthreats, their systems and cybersecurity defences.

People can be both a key risk to your cybersecurity management and a key defence. A simple and effective way to encourage positive behaviours is to raise awareness of the risks of cybercrime to both clients and staff and foster a ‘no blame culture’.

Training equips staff with the skills and confidence to recognise threats and manage confidential information appropriately. This does not need to be costly and many firms we saw took advantage of free training sessions and expert advice offered by their banks and insurers. Cybersecurity networks or groups can also help to maintain knowledge and identify any emerging risks on the horizon.

Alternatively, regular and collaborative awareness raising, built into meetings and every workday, can nurture an informed workforce who can manage risks and challenge others appropriately.

Q: Are your staff trained adequately, able to recognise risks and escalate them to the right people at the right time?

Carry out a heath check of your training regime. Keeping records of training undertaken can help you to assess whether there are any gaps in knowledge or whether training needs to be updated.

A cyberattack can affect anyone at the firm and training should just not be limited to senior members of staff or fee earners. The involvement of senior members of staff in cyber training can enhance its credibility and emphasise that you take cybersecurity seriously.

Sharing your experiences of both successful and unsuccessful attacks with staff, clients and even other firms encourages vigilance and can help others to know about emerging risks. A transparent approach to cyber security can help you to reinforce the idea that anyone, no matter how well resourced, can be affected by cybercrime and everyone is responsible for managing cyber threats.

Checklist:

Now, check your answers to the following questions:

- Have all staff, including the senior team, and support staff recently received training on cyber risks?
- Do you have a firm wide training schedule as well as individual training plans?
- Have you updated your training to include current cyber incident trends and specific risks facing your firm's network?
- Would staff feel confident to check any concerns about cyber incidents with senior staff or the IT team?
- Is your training relevant to your staff and practice areas?
- Do you test knowledge and learning outcomes?
- Do you cultivate a no blame culture and reward positive behaviours such as prompt reporting?
- Do you know what whitelisting is?
- Have you taken advantage of any free training or advice sessions available from your bank or insurance provider?

Policies and procedures

Having a tailored cyber security policy will help you and your staff protect your firm from cyber security threats. However, concerningly,14 of the 40 firms we visited did not have a specific policy on acceptable and secure use of the system, and nine firms did not have an IT security policy.

Furthermore, 23 firms had taken no steps to test or audit their processes and/or procedures. Eight firms did not have a written policy that explained whether removable media such as discs and data sticks could be used or how to use them safely.

In contrast, we identified that firms which had Cyber Essentials Plus accreditation were more likely to have good policies and procedures in place and had taken effective steps to protect the firm from any future incidents. We were also pleased to note that 80 percent of firms kept records of cyber incidents and could review and monitor trends and patterns.

Firm A

We visited a small firm that reported that they had transferred the proceeds of a house sale to hackers, following a phishing attack. The firm had an external IT consultant and introduced us to the individual who was their "Cyber Security Compliance Officer". The individual was a new trainee solicitor.

The officer had prepared several policy documents, however on closer inspection they were generic and included a blank risk assessment. The officer was unable to answer our questions about the phishing attack and the firm’s external IT consultants had to explain what the firm’s policies were in key areas.

After the meeting, we met with the fee earner who had been the subject of the original phishing incident. It concerned us that he was unable to fully explain the meaning of the term ‘phishing’.

Firm B

We visited another small firm that reported a similar phishing attack in a conveyancing transaction, but this time it was the client who transferred money to a fraudster purporting to be the firm.

The firm had detailed policies and procedures in place, tailored to the firm. They also kept records of all the cyber incidents that had occurred and were able to discuss in detail the number and nature of the attacks.

They had employed external IT consultants to manage their IT operations but were very knowledgeable about their systems and cyber risks. They had also undertaken Cyber Essentials Plus Training.

Diagnostic check-up: Policies and Procedures

We expect firms to have robust cyber security policies and procedures in place to mitigate against cyber risks. For example, having effective governance structures, systems and controls to make sure you comply with regulatory obligations and other legislative requirements[10 [#n10]].

Cybersecurity is not just an IT issue; it is a business wide concern that affects all staff and even your clients. It is therefore vital that senior managers take the lead with a knowledgeable and strategic approach to cyber policies and reporting requirements. We identified that only 70 percent of the firms we visited reported all successful cyber incidents to us. Our Enforcement Strategy[11 [#n11]] sets out our expectation that firms report attacks, even if there are no concerns about personal conduct or systems.

This is because it helps us to understand the threats firms are facing. However, if your firm is large and/or you routinely receive high numbers of unsuccessful attacks every day, we do not expect you to report every single one to us, unless it is particularly significant. We also identified that some staff did not always escalate cyber incidents such as phishing emails to relevant staff. Your policies should be tailored to reflect your own working practices and include practical information such as when and who to report cyber incidents to.

Q: Do you have adequate procedures and knowledge to protect your firm from cyber risks?

Carry out a health check of your policies and test whether they are being implemented as you expect and communicated to all staff effectively.

Having a good foundation of policies and procedures can help firms manage security risks while enabling flexible working practices and investment in innovative technology. Your policies should be a practical tool that identifies key risks, priorities, responsibilities and resources. They should be living documents that are reviewed regularly.

Some areas to consider include:

- tracking and recording cyber incidents so that you can detect trends and patterns, for example whether an employee or client is being targeted
- having policies for critical high-risk areas, for example removable devices and mobile working
- identifying clear reporting lines to build confidence in your procedures from the most senior to the most junior staff
- including protocols that determine when you report cyber incidents to the SRA, ICO, Action Fraud and the NCSC, depending on their seriousness.

Finally maintain your knowledge and that of your staff by keeping up to date with cyber threat trends and security guidance. For example, from your professional or specific cyber security networks, the NCSC, the Law Society and our scam alerts on Twitter. Share this information with your firm regularly.

Checklist:

Now, check your answers to the following questions:

- Do you encourage your staff to use strong, unique passwords?
- Does your system prompt staff to change passwords if they encounter suspicious behaviour?
- Have your password policies been updated in line with the NCSC's current password guidance?[12 [#n12]]
- Do you have a mobile working policy relating to safe use of systems and devices?
- Do you have policies on using removable media?
- Do you have protocols for deleting and disabling user accounts for ex members of staff?
- Do you have a policy to help staff understand how to use your systems safely?
- Do you have a dedicated senior member of staff to oversee your IT systems?
- Do you have clear reporting lines that staff feel confident to use when things go wrong?
- Do you encourage a culture of information sharing when risks arise?
- Do you keep records of cyberattacks and review to determine patterns and trends?

- Do you know when cyber incidents should be reported to the SRA and/or the ICO?

Technology

Several firms reported that their websites, systems or email accounts and the accounts of clients and third parties had been hacked by fraudsters. This included:

- a website which had been hacked for a short time by a political group
- a website subjected to a 'denial of service attack' (DOS) preventing access.
- mass phishing emails impersonating a firm sent from their email account to their contacts list following a cloud storage hack
- a firm who made an online payment on a bogus banking website.

Hackers exploit weaknesses in systems to gain unauthorised access. Therefore, it is vital to install updates known as ‘patches’ as soon as they are released and always use the latest version of operating systems and browsers.

However, we identified that only 47 percent of the firms we visited had an inventory in place that would enable them to check whether systems had been updated or needed to be replaced. This was concerning because 37 percent of the firms we visited were using Windows 7 operating systems which are no longer be supported with security and software updates.

Seventy five percent of the firms we saw used third-party IT professionals. These providers can provide valuable expertise that allows firms with limited resources to focus on their businesses. However, firms remain responsible for oversight of their cybersecurity. Two of the firms we visited were exposed to successful cyberattacks as a result of failings by their IT providers.

Case Study: Hacking by Brute Force

A conveyancing firm discovered that their password had been compromised. They believed this had been hacked by ‘brute force’, an attack where fraudsters attempt to force entry by guessing passwords using multiple attempts.

Once access to the system had been secured, the fraudsters set up a forwarding service from the fee earner’s e-mail account and intercepted various e-mails. Details within emails were then altered and the firm was conned into paying £13,000 to a fraudster. The issue subsequently came to light after the client raised concerns about the money with the firm.

Outcome

The firm discovered that their external IT provider had not configured the system to prevent multiple password attempts. Suitable security measures had not been switched on and the fraudsters were able to use software to crack the password by trial and error. In addition, the audit trail function had not been switched on and this allowed external individuals to access the system unnoticed.

Diagnostic check-up: Technology

No system or security is infallible, but firms should take reasonable steps to maintain a secure IT environment. Firms should consider their computer network in its entirety. A weak link in the chain will undermine the whole system and could result in loss of client money or a breach of confidentiality.

Basic maintenance regimes such as updating operating systems, firewalls and anti-virus software as well as keeping up to date with current cybercrime trends can help your firm defend against cyberattacks.

Take steps to protect clients from the risks of cyberfraud so that they can have confidence in the services you provide by carrying out due diligence into outsourced service providers and IT professionals.

Cybersecurity is ultimately a broader risk than the use and maintenance of technology alone. You or your senior management team should have suitable knowledge and oversight to ensure a strategic approach to technology and security across the whole firm.

Q: Would your cyber security measures meet the standards we expect?

Carry out a health check of your systems and identify whether there are any security gaps by completing a system inventory of your assets and carry out a risk assessment of how well client data and money are protected.

Managing risks

Checklist:

Now, check your answers to the following questions:

- Do you maintain an inventory of your assets and review your systems regularly?
- Have you got anti-virus software installed on all systems?

- Have you checked that all software is up to date and not subject to vulnerabilities?
- Have you or your IT support checked whether your website or firm name has been compromised?
- Have you ensured that IT devices are physically secure both on and off site?
- Have you updated your mobile devices with two factor authentication?
- If you use Office 365, have you configured it to defend against cyberattacks?
- Do you monitor systems to detect unauthorised access or dangerous websites?
- Do you control user access to job roles or limit apps which can be used by staff?
- Have the default settings on your systems and WIFI router been updated?
- Are your laptops and mobile devices encrypted?
- Do you limit administrator access to staff who are required to make changes?

Firms were often left with costly consequences following a cyberattack. We identified that over £4 million in client money had been stolen from just 23 of the firms we visited. This was a shortage that needed to be replaced by firms immediately. This was not the only financial consequence for firms. Other effects included the time taken to deal with the incident, paying the excess on insurance claims or upgrading security and IT systems. In many cases, the repercussions were reputational, time consuming and even had an impact on staff morale.

One firm we met found that their professional indemnity insurance (PII) did not cover client losses resulting from cybercrime. Another firm in our sample are still in dispute with their insurance provider several months later about whether they were covered for cybercrime losses. Just 30 percent of firms we met had specific cyber insurance.

Most firms we visited responded positively to cyberattacks by reviewing and/or introducing new policies, technology and training. However, not all firms in our sample took active steps to review their procedures and protect their firm after a cyber incident. Cybercrime is a developing risk and as such, opportunities to evaluate and manage the likelihood of future threats should not be missed.

Firm A: Failing to mitigate phishing email risks

The firm had been subject to an email modification scam that originated from the client's email account. The firm transferred completion funds to a fraudster's bank account. The firm explained that they had not made any changes to their policies and procedures as a result of the attack but had raised awareness about the attack and reiterated what their policy

was. They did not keep records of any cyber incidents but felt the weakest point in their security were their clients.

We met with a fee earner to discuss their experiences of the firm's cybersecurity measures. The fee earner explained during the meeting that he had in fact received a phishing email earlier that day purporting to be from a client of the firm. When we asked what he did about this, he explained that he simply deleted it.

We met with a fee earner to discuss their experiences of the firm's cybersecurity measures. The fee earner explained during the meeting that he had in fact received a phishing email earlier that day purporting to be from a client of the firm. When we asked what he did about this, he explained that he simply deleted it.

Firm B: Mitigating phishing risks appropriately

A first-time buyer wanted to send a deposit of £7,500 to the firm. The firm told the client that they would let her know when it should be paid. Shortly afterwards, the client received an email purportedly from the firm at 2:30am asking her to transfer the deposit into the firm's bank account. The client complied with the request and transferred the money to the fraudsters.

The firm immediately checked and secured their systems and controls. Additionally, their external IT company spent time with the client checking her computer and making it secure at no cost to her.

We expect firms to run their business on sound risk management principles and 'identify, monitor and manage all material risks'.[13 [#n13]] Managing risks is a business-critical issue for firms of all sizes. It can start with some basics, such as understanding your business, identifying key risk areas, learning from previous incidents and planning how to manage future threats.

Q: Have you taken steps to protect your firm?

Carry out a health check of your systems, policies and procedures every time you are subject to a cyber incident and reflect on whether this has highlighted any gaps in your security. Evaluate your risk areas with a risk assessment and check any vulnerabilities. Three key steps to consider are:

People: Ensure that the right people are placed in positions of responsibility and have the knowledge and skills to manage cyber risks. This is a firm wide issue and ideally a senior manager or the Board should have direct strategic responsibility for managing cyber risks. Departmental cyber security targets or even competitions can keep staff

engaged in the process of maintaining a secure environment and encourage them to take responsibility for reporting risks.

PII: Check your PII policy. The minimum terms and conditions may cover losses of client money from cybercrime, limited to the amount insured. Firms should consider whether they have adequate cover from their existing PII for client's or their own losses resulting from cybercrime. Failing to have suitable cover could have severe consequences.

Pay: A specific budget allocated to cyber security allows you to invest in new technology and implement contingencies when system failures arise. However, using the free resources provided by the NCSC is also a good start to assessing whether your controls are suitable.

First steps to manage cyber risks

Five areas to focus on if you are starting to think about improving your cyber security are:

- Update your knowledge
- Patch software and monitor malware defences
- Support and motivate staff
- Plan for future threats
- Have effective cyber management oversight

Checklist:

Now, check your answers to the following questions:

- Have you reviewed and updated your policies after successful cyberattacks?
- Is cyber security a standing agenda item in management meetings?
- If relevant, does a senior member of the board or management team have direct responsibility for cyber security?
- Have you updated your operating systems and devices to one that receives regular security updates and has a built-in malware protection tool?
- Have you reviewed password security and made changes to default passwords?
- Do you regularly back up data and keep this in a safe and secure location?
- Do you have a strategy to monitor your systems and network?
- Do you keep up to date with cyber risks and threat alerts from the NCSC?
- Does your PII cover losses from cybercrime?

Now check your answers back.

Are you confident that your firm is on target to be cyber secure?

Annexes

Open all [#]

Annex 1: Resources

Do you want to know more about our thematic review of cyber security at firms? Click here to read our detailed Thematic Review of Cyber Security [https://consultations.sra.org.uk/sra/how-we-work/archive/reports/cyber-security/] . A glossary of common cyber terms to demystify cyber security and cybercrime (Appendix 1. Link)

Further Reading:

- Trends in cyber security breaches [https://www.gov.uk/government/publications/cyber-security-breaches-survey]
- SRA Risk Outlook [#]
- Law Society Cyber Security Guidance [https://www.lawsociety.org.uk/support-services/practice-management/cybersecurity-and-scam-prevention/cybersecurity-guidance-and-advice/]
- National Cyber Security Centre [https://www.ncsc.gov.uk]
- Cyber Essentials [https://www.cyberessentials.ncsc.gov.uk/advice/]

Cybercrime	
Brute force attack	Fraudsters use software to crack passwords by trial and error, inputting many combinations to gain access.
Cyber incident	A breach of a system, usually to gain malicious unauthorised access by a wide range of means.
CEO fraud	Criminals impersonate a senior figure at a firm usually by using a very similar modified email address, to impose authority and encourage recipients to send money. See also 'Whaling'.
Denial of service (DoS)	A technique where multiple systems are used to perform a cyberattack usually on a website, overwhelming the service.
Email modification fraud	Criminals intercept and falsify emails between a client and their firm, leading to bank details being changed and money being lost.
Hacker	Someone who breaks into computers, systems and networks.
Keyboard logger	A virus or physical device that logs keystrokes to secretly capture private information such as passwords or credit card details.
Malware	Short for malicious software, it is often contained within a website link or attachment and includes

	viruses to disrupt or access, ransomware and worms for example.
Man-in-the-middle-fraud	A fraudster intercepts an email communication and alters it before sending it on to the recipient.
Phishing	An untargeted cyberattack in which emails are sent on mass to users usually to illicit sensitive information, such as passwords and bank details.
Ransomware	Ransomware is a type of malware (malicious software) which encrypts all the user's data blocking access to all or parts of their systems.
'Smishing' or SMS Phishing	A phishing attack but using an SMS or text message on a mobile phone to obtain sensitive or personal information by impersonating a reputable company and encouraging the recipient to access an embedded web link or call a telephone number.
Spear Phishing	Another form of phishing attack but one that is targeted to gain information usually by using email modification fraud.
Spoof email	Also known as email modification fraud. An e-mail with a forged sender address usually so that it appears to have originated from someone the recipient knows.
Spyware	Malware that enables a fraudster to monitor or capture information from a user's system such as passwords and credit card details covertly. For example; 'adware'.
Supply chain compromise	Information from third parties involved in a transaction can be intercepted and the fraudster uses this to attack when funds are transferred. Anyone in the chain can be targeted including clients.
Vishing	Phishing by voice is the fraudulent practice of making phone calls purporting to be from reputable organisations to induce victims to disclose information, such as bank account details.
Water holing or watering hole	A fake or infected website used by hackers to target specific users.
Whaling	Targeted modified emails impersonating senior employees at an organisation which are then sent to other employees to obtain information or money. Also known as CEO fraud.
Worm	Malware that spreads across a computer network by replicating itself.

Annex 2: The Cyber Security Glossary

Cyber Security

Administrator account	A user account that allows you to make changes that will affect other users. Administrators can change security settings, install software and hard ware and access all files.
Antivirus	Antivirus software is used to monitor a computer or network, to detect cyber security threats ranging from malicious code to malware.
Backing up	To make a copy of data stored on a computer or server to lessen the potential impact of failure or loss.
CyberEssentials [https://www.comtact.co.uk/blog/cyber-essentials-vs-cyber-essentials-plus-whats-the-difference]	A Government supported scheme designed to help you protect your organisation against cybercrime.
Data server	A computer or program that provides other computers with access to shared files over a network.
Disaster recovery plan/ incident report plan	An inventory of an organisation's hardware and software and a plan to make sure that all critical information is backed up and contingencies if any losses occur.
Firewall	Hardware or software designed to prevent unauthorised access to a computer or network from another computer or network.
Information security policy	Usually the result of a detailed risk assessment, they are a group of policies and practices that form a firm's strategy for managing specific risks and protecting information.
National Cyber Security Centre (NCSC) [https://www.ncsc.gov.uk/]	A government organisation that provides advice and support to the public and private sector about cyber security.
Router	Device that directs messages within or between networks.
Sandboxing	A sandboxed application is run in an isolated environment with restricted access to the rest of

	your device and network to protect it from malware.
Server	A computer programme that provides services to other computers over a network.
Two-factor authentication	The use of two different components to verify a user's identity.
Virtual private network (VPN)	A private network that secures and anonymises your network address across different locations that cannot access or be accessed by other users of the wide area network.
Whitelisting	An administrator can limit the access users have to applications on a device or computer.

Notes

1. Rule 6.1 SRA Account Rules 2019
2. https://www.sra.org.uk/risk/outlook/risk-outlook-2020-21/client-money/ [https://consultations.sra.org.uk/archive/risk/outlook/risk-outlook-2020-21/client-money/]
3. https://www.wearepay.uk/ [https://www.wearepay.uk/]
4. https://www.sra.org.uk/solicitors/guidance/ethics-guidance/third-party-managed-accounts/ [https://www.sra.org.uk/solicitors/guidance/ethics-guidance/third-party-managed-accounts/]
5. A sole practitioner’s PII was refused on the grounds that she had effectively ‘condoned dishonesty activities’ following a vishing attack in 2015. Her firm was intervened into in 2016 when she was unable to replace the resulting client shortage of £750,000.
6. Domain Message Authentication Reporting and Conformance
7. Paragraph 2.9 SRA Code of Conduct for Firms 2019
8. https://ico.org.uk/media/for-organisations/documents/2614816/responding-to-a-cybersecurity-incident.pdf [https://ico.org.uk/media/for-organisations/documents/2614816/responding-to-a-cybersecurity-incident.pdf]
9. Paragraph 4.3 SRA Code of Conduct for Firms 2019
10. Paragraph 2.1 SRA Code of Conduct for Firms 2019
11. https://www.sra.org.uk/sra/strategy-2017-2020/sub-strategies/sra-enforcement-strategy [https://www.sra.org.uk/sra/strategy-2017-2020/sub-strategies/sra-enforcement-strategy]
12. https://www.ncsc.gov.uk/collection/passwords/updating-your-approach [https://www.ncsc.gov.uk/collection/passwords/updating-your-approach]
13. Paragraph 2.5, SRA Code of Conduct for Firms