Solicitors Regulation Authority

Cyber Security - A thematic review

Published 2 September 2020

Download: Cyber Security - A thematic review (PDF 33 pages, 544KB) [/globalassets/documents/sra/research/cyber-security-a-thematic-review.pdf?version=4a48a2]

Executive summary

Introduction

On a day-to-day basis, law firms handle financial transactions involving large amounts of money and send and receive sensitive client information. Much of this activity takes place digitally, be it online bank transfers, automated identity checks or simply emailing financial and personal information between law firms and clients.

We have warned the profession about the dangers and need to be vigilant against cybercrime for a number of years. Whether by use of spyware, identity theft, viruses or simply tricking people to reveal sensitive data, cybercriminals are always attempting to find new victims and weaknesses in defences they can exploit.

With Covid-19 meaning millions more people than ever before are working remotely and carrying out both personal and business activities online, the need for everyone to remain extra cybersecurity vigilant is arguably greater than ever. We have already published key support resources including a dedicated Q&A on cyber security [/news/news/cyber-security-qa/] as firms and solicitors change the way they work.

Effective cybersecurity is not just a technological issue, or simply about having the latest security software in place. In fact, the biggest vulnerability - and also potentially best defence - most companies will have regarding cybercrime lies in the day-to-day practices and awareness of their people.

We know the majority of solicitor firms are aware of the risks and have developed processes and approaches to try and make sure they don't fall victim to the criminals. But attacks still happen, and even where a firm thought they were secure, some unfortunately are still successful.

And while law firms usually have insurance to protect against financial loss, the cost of cybercrime can be about more than just money. Where clients are involved, even if the money is eventually recovered, the impact and stress of being involved in an incident can be significant. For

a firm there can be significant reputational, resource and longer-term financial impacts of being caught up in cybercrime incident.

Purpose of review

We wanted to know more about the experiences of firms that had been targeted by cybercriminals. We wanted to learn more about what types of attacks they were subjected to, what measures they did/did not have in place to protect themselves at the time and how being targeted affected them. This included assessing the mitigation firms introduced to reduce the risk of a repeat incident.

To do this we selected a sample of 40 firms to visit and interview about their experiences of cybercrime. The firms had all reported that they and/or their clients had been targeted by cybercriminals over the previous three-year period.

What we found

This report outlines our findings in five key areas:

- cyberattacks – type, volume and impact
- people – what support was provided to staff?
- technology – what controls did firms have in place?
- support – what support did firms use?
- reporting – did firms meet their reporting requirements?

Cyberattacks

Three quarters (30) of the firms we visited reported that they had been the target of a cyberattack. In the remaining ten cases, firms reported that cybercriminals had directly targeted their clients during a legal transaction.

While not all incidents culminated in a financial loss for clients, 23 of the 30 cases in which firms were directly targeted saw a total of more than £4m of client money stolen. While £3.6m of this was ultimately claimed against insurance policies, a further £400,000 had to be repaid directly from firms' own money. These figures do not take account of the wider cost of such incidents to firms, for example higher insurance premiums, lost time and damage to client relationships.

The financial impact of a loss of data is more difficult to calculate, but we found these often resulted in indirect financial costs. For example, one firm lost around £150,000 worth of billable hours following an attack which crippled their system.

Firms also reported that attacks were not isolated incidents. Two of the larger firms we visited reported that they were targeted hundreds of

times a year, although the vast majority of these attacks were not successful.

Cybercriminals typically used a broad range of approaches when targeting their victims. The most common methods included:

- email modification
- spyware
- ransomware
- viruses
- denial of service attacks
- gaining remote access to a firm's systems.

People

Ultimately most cyberattacks target people. Cybercriminals use technology to trick their victims into sharing confidential information and provide access to their funds. Accordingly, 60% of the firms we visited said they felt their biggest potential vulnerability to cybercrime was linked to the knowledge and behaviours of their staff.

Despite this, we still found that only around two-thirds of staff in the firms we visited claimed to be 'knowledgeable' about cybersecurity and IT issues, with even some senior figures unable to answer basic questions about cybersecurity terminology.

For firms, having knowledgeable and empowered staff is the first line of defence against cybercrime. Creating such a culture relies upon having effective policies and controls in place. Of the firms we visited, we concluded that 11 had inadequate policies in place, and 10 had inadequate controls.

Eight firms (20%) we visited had never provided specific cybersecurity training to their staff. More than half did not keep records of who had received such training.

We also reviewed the steps firms took to remedy the causes of historical incidents to avoid similar issues occurring in the future. Most firms implemented appropriate mitigation measures and the remainder were still implementing new processes and controls. Inevitably, mitigation cost firms time and money.

However, for most firms, the cost of the mitigation was less than the amount of money lost. This highlights that security measures often make sound business sense as well as being a regulatory requirement.

Technology

Our review also evaluated the technological controls that firms had employed. While most firms had introduced adequate and appropriate

systems, some firms found this a confusing area.

Reassuringly 93% of the firms we visited confirmed they had firewalls in place (the remainder were unsure), with more than half having firewalls round both individual devices and a wider firewall round their overall systems.

All the firms we saw confirmed that their laptops and devices were password protected. Moreover, 25 confirmed that two-factor authentication was required from staff/clients when engaging in many day-to-day activities.

All firms undertook some form of data backup exercise, while the majority (87%) were able to show they made active use of anti-virus software. We did however find other practices that were commonplace which could potentially make a firm's systems vulnerable. These included:

- more than half of firms allowed external data sticks to be freely used and plugged into their machines
- two firms used an old Windows operating system for which security updates had ceased in 2014, while 16 were using a system for which Windows support was due to end imminently.

This is significant because cybercriminals will exploit weaknesses in systems to gain unauthorised access. The best defence is to avoid the use of data sticks, to install updates known as 'patches' as soon as they are released and use the latest version of operating systems and browsers.

We were particularly interested in each firm's ability to respond to a catastrophic cyberattack. Twenty-seven firms (68%) had a disaster recovery plan in place, but 15 of them also admitted that the document was stored on the same system that would be the target of any attack. In contrast, 19 firms had employed specialists to stress test their systems.

Support

In terms of IT/cyber security support three quarters of firms predominantly relied on help from commercial IT specialists. While we identified that this can be a source of valuable expertise for firms, they should be careful not to become totally reliant on this.

This point was highlighted by two firms that had received poor advice from third-party providers, which ultimately left the firms exposed to fraudsters.

In terms of wider/specialist support we also found that:

- 12 firms had specific cybercrime insurance

- seven firms were part of specialist cybersecurity networks/forums
- five firms had Cyber Essential Plus certification, with 16 further working toward this.

Cyber Essential Plus is a Government-supported scheme designed to help businesses protect themselves against cybercrime.

We found that firms with Cyber Essentials Plus accreditation were more likely to have good policies and procedures in place and have taken effective steps to protect themselves from future cyber security incidents.

Reporting

When issues occur, we expect firms and individuals to take appropriate steps and comply with their regulatory and legal reporting requirements. This includes their duties to report incidents to the SRA.

We found:

- 73% of firms (29) had reported incidents to us
- seven significant incidents were not reported, despite clear and significant breaches
- reports were not routinely made when clients were affected but the firm had not been directly involved, for example, where clients were tricked into sending money to a third party.

Although reporting where only clients are affected is not a regulatory requirement, we encourage reporting as the information might be useful in helping our wider work to tackle cybercrime and raise awareness of common scams.

Certain cybercrime incidents involving personal data need to be reported to the Information Commissioner's Office (ICO) within 72 hours. While this is now a mandatory requirement, previously it was not. We spoke with firms about their ICO responsibilities:

- Nine firms had made a referral to the ICO following a cyberattack.
- Nine firms encountered an incident where it appeared personal data had been accessed but no report had been made.

Twenty-three firms had informed law enforcement following their last cybercrime incident. These included incidents where:

- a client transferred £70K to a fraudster
- a further £70K transfer was made to a fraudster in an unrelated incident by another client
- a solicitor transferred £340K to a fraudster.

Going forward

Our review shows that cybercrime is indiscriminate. No businesses are safe, with criminals targeting firms and transactions across all areas of legal sector.

Fortunately, firms also demonstrated that there were numerous simple and effective ways to reduce their exposure to cybercrime risks. However, in order to do this meaningfully, firms must understand the risks they face.

Significantly, most firms believed that staff were the greatest cyber risk and this reflects our conclusion and findings. A distracted, inexperienced or disgruntled member of staff can enable and allow substantial, business-threatening cyber-security breaches. This can be compounded where a system or control is poorly configured or designed. Like most risks, firms should consider how incidents might occur and what mitigation could be used to contain and minimise an initial breach.

Cyber security is an issue for any process which is wholly or partially reliant on technology, including those facilitated online, via email or through the use of any computer or device. However, ultimately it is a broader risk than the use and maintenance of technology alone. Firms need to have suitable knowledge and oversight to ensure they maintain a strategic approach to technology and security across the whole firm.

Cybercrime is a constant threat for everyone and all the more so as we all rely on technology as we adapt to new ways of working against the backcloth of Covid-19 . There is a wide range of support available to firms and it is all the more important that firms take the steps needed at the moment.

> "Cybercrime continues to rise in scale and complexity, affecting essential services, businesses and private individuals alike. Cybercrime costs the UK billions of pounds, causes untold damage, and threatens national security."
> National Crime Agency, 2019

Open all [#]

Cyber-attacks

Type of incidents

Firms must protect both clients' funds and data[1] [#n1]. In addition, firms have a statutory duty to protect data against "unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures[2] [#n2]."

Although most incidents we reviewed featured fraudsters deliberately targeting specific individuals and client money, we also saw

indiscriminate attacks. These appear to have been designed to harvest and control firm data. An adequate security system must therefore consider the threat to both client money and client data.

Firms had encountered a broad range of malicious software (malware) designed to disrupt computer operations, gather sensitive information or gain access to private computer systems. This included:

- email modification fraud/phishing/vishing where individuals were lured by spoof emails and phone calls into providing sensitive information about themselves or clients, such as passwords or banking information. This was the most common cyber-attack experienced by our firms and their clients
- spyware which allow unauthorised parties to view computer use in real time
- ransomware which prevented access to all or some firm data until a ransom had been paid
- viruses which destroyed or manipulated computers and data
- denial of service attacks which were used to target and block access to strategic websites
- web shells where criminals gained remote access to a firm's systems
- man-in-the-middle fraud where criminals inserted themselves in between the client and the firm to intercept communications and manipulate correspondence and interactions.

Significantly, our ability to report on this area is hindered because a large minority of firms were unable to explain what had happened and often confused basic types of cyber-attacks.

Most incidents occurred due to individual errors and misunderstanding rather than systems being hacked. This distinction is important. Many of the individual errors could have been easily avoided with more time and effort rather than expensive equipment. We saw very few incidents that involved an element of hacking.

Volume of incidents

In September 2019, Action Fraud reported an annual total of 43,717 referrals about fraud and cybercrime. They consider this to represent a fraction of the incidents that take place and the National Crime Agency think the issue is likely to grow:

> "Off the shelf' tools mean that less technically proficient criminals are now able to commit cybercrime and do so as awareness of the potential profits becomes more widespread. The evolving technical capabilities of malware means evolving harm as well as facilitating new crimes[3 [#n3]]."

We were interested to find out more about the volume of attacks that firms endured. We asked firms how many times they had been targeted since 2016. The figures below indicate whether each firm recorded any attacks during the period, regardless of how many times they may have been targeted:

Interestingly:

- 75 percent (30) of the firms told us that they had been targeted during the three-year period
- two large firms were targeted more than 100 times each year. The remaining 28 firms had recorded a combined number of 65 attempted attacks
- 31 attacks had been successful.

However, these figures only represent a part of the picture:

- each member of the sample was selected because we had received a substantive cybercrime report about them or their clients
- nine firms told us that they did not collect data in this area.

These figures raise interesting questions about how and when firms record data about cyber-attacks. Inevitably, this effects our ability to provide accurate data about the experiences of the profession. Further information about firm reporting is covered below.

Impact

Thirty-one firms had been successfully targeted by fraudsters and the results were often catastrophic. We looked at three specific areas:

- immediate aftermath
- repercussions
- mitigation.

Immediate aftermath

Twenty three firms had made an initial insurance claim following the loss of client or office money. In total, firms were required to repay £4,059,689 to clients. This included:

- £3,665,799 paid out by insurers on behalf of sixteen firms
- £393,890 paid out in total by eighteen firms.

Repercussions

A loss of client money or data is only one aspect of a successful cyber-attack. We asked the 23 firms who had experienced a financial loss about

any further repercussions they had experienced. Firms experienced issues that often had an impact on their operational capabilities and further hidden financial implications.

Loss of time includes time spent by firms repairing and improving their IT system, investigating incidents and dealing with insurance claims. Often these activities were at the expense of the billable hours of senior management.

In some cases, repercussions had significant life changing consequences including:

- long term stress and debilitating anxiety
- impacts on ability to retire
- firings and demotions.

We were concerned that some firms did not foster a supportive, no-blame culture. The ability to respond to a cyber-attack quickly may allow a firm to mitigate the severity of any outcome. A punitive response by a firm might influence a staff member's future actions and undermine their willingness to identify and report future cyber risks. It is important that firms focus on encouraging positive behaviours and raising awareness rather than apportioning blame.

Mitigation

Firms also introduced mitigation to try and prevent similar future attacks. Mitigation fell into three broad categories:

- controls – any measure that physically prevented the incident from reoccurring
- process – any measure that determined a course of action
- policy – any measure which outlined a firm's expectation or requirement.

The following table illustrates how many of the 40 firms reviewed introduced new/changed mitigating approaches following being targeted. Twenty three of the firms introduced more than one measure:

We judged that the mitigation introduced appeared to be effective and appropriate in 92 percent of the matters we investigated. The remaining incidents were still being resolved by firms.

We asked firms how much the mitigation measures had cost:

Twenty seven attacks had resulted in firms losing office or client money. All but one firm introduced mitigation that they believed would prevent a similar event from occurring. On 62% of these occasions, the cost of the mitigation was less than the initial loss incurred by the firm.

People

Knowledgeable and empowered staff are the first line of defence against cybercrime.

An ill-informed member of staff can be catastrophic for a firm. Most firms told us that their staff were the main vulnerability in any system. We asked firms about their greatest cyber risks:

- 60 percent told us it was staff knowledge and behaviour
- 30 percent told us it was client knowledge and behaviour
- 33 percent specifically considered e-mail interception as one of their greatest risks.

We met with each firm's nominated cyber security lead and a separate fee earner. The nominated cyber security lead was typically a senior figure at the firm. We were interested in each interviewee's perceptions and level of knowledge:

We compared this with the corresponding firm's policies and controls. Were perceptions about knowledge reflected in better policies and controls?

We ultimately concluded 11 firms had inadequate policies and 10 firms had inadequate controls. Interestingly in some of these cases this was despite the firm feeling senior colleagues were knowledgeable about cyber security and IT issues.

This data suggests a minority of people either knowingly accept poor policies and controls or alternatively overestimated their degree of knowledge. This is particularly significant because an ability to assess a risk (and implement an appropriate mitigation) is dependent on your level of knowledge and understanding.

Once firms acknowledged staff and people as their greatest vulnerability, we were interested about how firms mitigated this and fostered an appropriate culture. We wanted to understand how firms:

- role modelled appropriate behaviours
- upskilled staff

- supported staff via meaningful processes and controls
- tackled worst case scenarios.

Knowledge

The ability to prevent and mitigate cybercrime depends on everyone within a firm having a general level of knowledge about the topic.

We were interested in whether individuals understood the basics and asked interviewees whether they understood and could explain basic terms. While the overall majority of staff could explain the terms, the majority of senior figures could not:

These findings raise questions about the ability and role of senior figures in responding meaningfully to cyber security issues. While we accept firms may seek external help and guidance, a basic understanding at all levels in a firm is a necessity.

These findings were exacerbated (dramatically in some cases) when we asked fee earners a similar set of questions:

The first step to mitigating a risk is to understand it. Our findings raised concerns. Ransomware is typically an indiscriminate attack and all staff are likely to be targeted. One firm told us that around £150,000 of billable time was lost due to a ransomware attack initiated accidentally by a fee earner.

Supporting individuals and promoting the right behaviours

We explored how firms supported staff and encouraged sensible decision-making.

We were specifically interested in the following areas:

- figurehead – who is responsible for cybercrime at the firm and what do they do?
- training – who is trained?
- processes – what processes are in place and are they adequate?
- controls – what controls are in place to promote appropriate behaviour and minimise critical issues?
- worst case scenario – how do firms control situations?

Figure heads

An influential and visible leader will help set the tone, support decision making and outline expectations.

We asked firms who was responsible for cybercrime in their business.

- 67 percent of firms had delegated responsibility for IT to a specific person
- 40 percent of firms had a dedicated internal IT team
- 75 percent of firms had help from an external IT team.

During each visit, we spoke with the individual who was responsible for the firm's IT security. Inevitably, these individuals had a broad range of skills and professional backgrounds:

We were interested in the influence that these individuals had on their firm. Reassuringly:

- 98 percent of the staff knew who was responsible for cyber security and cybercrime incidents
- 63 percent of the staff had sought advice and guidance from the nominated individuals.

We were also interested in the reporting structure at each firm. A systematic and formalised approach to risk and reporting, promotes record keeping and data analysis. This information should be escalated and used to support business decisions and prioritise expenditure and effort. Firms did this to varying degrees:

- 24 firms told us they responded to incidents as and when they occurred. It is our experience that providing ongoing time and space to discuss a risk will help firms act appropriately
- 16 firms had a defined escalation process for incidents
- 15 firms provided the information to a board or group of managers to monitor, record and respond to trends and incidents.

We also asked whether information was collated and logged:

- 11 firms did not keep basic information about cyber attacks
- Eight firms did not monitor attempted cybercrime issues
- 24 firms did not keep a specific incident log
- despite telling us that they kept a log, seven firms were not able to provide basic information about cyber issues.

If firms do not monitor and formally record the information, it is difficult to see how they take informed decisions.

We also asked specific questions about each firm's cyber security budget. A budget helps a business to plan and can establish goals and set priorities. It also encourages ongoing reviews and expenditure. By

upgrading software and hardware on a rolling, budgeted basis, firms can avoid ad-hoc, unplanned, crisis-driven expenditure. While all firms said they were willing to spend money on cyber security, only five firms had a specific annual budget for cybercrime detection and prevention.

Training

Cyber security risks are constantly emerging and developing. The provision of training is one way that firms can seek to frustrate fraudsters.

We asked firms about the frequency and type of training provided. We also wanted to know when training had last been provided:

The twenty percent of firms who had never provided specific cyber training tended to either incorporate cyber concerns into other training or minimise a risk through a process.

Significantly, cybercrime is a risk for the entire firm and fraudsters will target people across the business. As the National Cyber Security Centre acknowledge [https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/get-basics-right-risk-management-principles-cyber-security] :

> "Many cyber-attacks use indiscriminate scatter-gun approaches to targeting victims."

Firms told us about various incidents that featured administrative support, , finance and IT staff. Therefore, it is important that the training is provided to the entire business. However, this was not always the case at the firms we visited:

Firms offered a mixture of training formats:

Disappointingly, only 24 firms had kept a record of who had received training. Records are important and help firms to monitor and enforce training requirements.

Training will help a firm define its culture. It sets expectations and raises awareness among staff. This will be compounded by how firms respond when things go wrong. One firm had fired one individual and demoted another. While this may be appropriate,, firms also have to consider the impact on the willingness of others to raise concerns. A no blame culture may support people to come forward and raise issues and mistakes

promptly. This is significant because a quick response may help the firm to control and mitigate the impact of the attack.

Processes

Processes provide people with instructions and guidance. By providing clear expectations and outlining staff obligations, the firm can influence and support staff to make sensible decisions.

We were interested in whether firms had specific policies for set areas:

The vast majority of the policies we reviewed had been monitored and updated to reflect emerging trends and information. Firms had also developed other policies about:

- cyber security
- website and social media policies
- card payments
- email usage
- passwords.

Firms also implemented policies and procedures to help control client-based risks. Clients are an integral part of any process and firms should consider the risks that they pose. Firms addressed this risk by:

- telling clients that bank details wouldn't change
- not providing bank details by e-mail
- asking clients not to send money until it was requested
- reminding the clients about their use of social media and the information they share – for example information about a house move could potentially be used by fraudsters to manipulate others, for example solicitors or estate agents.

Significantly, any policy must be adequate and appropriate. We were not satisfied with the extent and/or details of policies at 11 firms and raised this directly with those firms. A poor policy is an inherent risk and is likely to leave the firm vulnerable.

Policies, processes and systems should be reviewed and maintained regularly to make sure that they remain effective and proportionate to the risks. Where possible, this should be done by an independent individual. The person could be independent of the process or the firm and this will help to generate an objective perspective. We found most firms could improve the degree of audit undertaken and noted that 23 firms had never had their IT policies and/or processes audited.

Worst case scenarios

No system or process is perfect, and firms should consider and prepare plans and actions to help mitigate incidents. As the National Cyber Security Centre states [https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/get-basics-right-risk-management-principles-cyber-security] :

> "Cyber security is as much about knowing how your organisation functions as it is about technology. Think about what people, information, technologies and business processes are critical to your organisation. What would happen if you no longer had access to them (or if you no longer had control over them?)."

As many firms told us, the ability to respond quickly to emerging events can significantly impact on any outcome.

We saw various attempts to prepare for incidents:

- 27 firms had produced disaster recovery plans. These varied in scope and detail. We recommend that firms take time to compile useful information (including contact details and telephone numbers) and document emergency processes. Significantly, firms must also consider where they keep the document. Fifteen firms stored the document on the same system that they predicted may be unavailable
- 19 firms had undergone penetration testing by an external party. These tests were carried out at a distance by specialists and were designed to test the security, vulnerability and robustness of the firm's software, hardware and security systems
- 15 firms had taken internal steps to stress-test processes and procedures, for example by undertaking mock-cyber incidents or testing staff responses to phishing enquiries. Findings and observations were then used to adapt and develop processes and training.

Significantly, 14 firms had taken no steps to test or audit their processes and/or procedures. This is a concern.

Firms should also consider the extent of their ability to manage and enforce proper staff practice and whether their arrangements are sufficiently robust to deal with wilfully disruptive staff. We found:

- 4 firms did not include security and confidentiality clauses in their contracts of employment
- 5 firms were not sure about whether they had any contractual protections or requirements.

The ability to enforce a firm's policies and processes are significantly enhanced where employment contracts stipulate specific powers and controls that are available to the employer firm.

Technology

If technology is understood and used appropriately, it can make it more difficult to target a firm. Cyber Essentials suggests a base layer of five technical controls [https://www.cyberessentials.ncsc.gov.uk/advice/] :

- use a firewall
- review and implement security settings such as passwords and two factor authentication
- control who has access to your system
- protect yourself from viruses and other malware
- keep systems up to date.

We were interested to find out more about the protections implemented by firms.

Firewalls

A firewall is a security device that provides a barrier between a computer or system and other external networks, for example the internet. It monitors and controls incoming and outgoing traffic and will automatically allow or block specific traffic based on predefined rules.

A firewall can be:

- software or hardware
- personal or a dedicated boundary firewall which protects an entire network.

Personal firewalls are often provided as standard with laptops and computers.

We found 93 percent of firms had a firewall in place (three firms were not sure whether they had any firewall). Firms used different types of firewalls:

We also asked firms about the configuration of their firewalls:

Although it is unlikely that firms do not have an active firewall, any risk is exacerbated by a general lack of knowledge and understanding about the mitigation.

Where a default password is supplied with any software or hardware it should be changed:

Again, people should understand the basics about how software and hardware to gauge whether the control is useful and adequate. A default password is not a password.

Reviewing and implementing security settings for devices and software

Securing systems and data is the core concept behind cyber security. We were interested to see whether firms had adopted obvious, basic measures such as passwords and two factor authentication.

Initially, we asked firms and staff whether they had read the National Cyber Security Centre's guidance on passwords. This information is free and developed by cyber security specialists. The responses and contrast between senior figures and staff show a similar pattern to the one demonstrated on our earlier question on knowledge and understanding:

The four fee earners who had read the guidance were working at firms where the management had also read the guidance. This emphasises the role of management in setting the tone for cyber security.

We also asked firms basic questions about their security settings:

- all firms told us that their laptops, desktop computers, tablets and smartphones were password protected
- 31 firms (78 percent) of firms used software to prompt password changes at specific points and dates
- 4 firms (10 percent) required a fee earner to share a password to carry out an aspect of their role
- 6 fee earners (15 percent) mentioned that they had received specific training about passwords
- 5 fee earners (13 percent) received no training or guidance from their firm.

Setting appropriately complex passwords is an intrinsic and important part of cyber security. In the 31 successful attacks we saw, weak passwords were cracked on four occasions. This included fee earners voluntarily providing information about their passwords to fraudsters and hackers using software to crack passwords by 'brute force'. This is where unauthorised individuals use software to identify passwords and gain unauthorised access to a system.

Importantly, firms should physically review the security on each system. While every firm said they employed passwords, one visit featured the discovery of a computer that could be accessed without a password. It subsequently provided full access to the firm's entire system. This highlights that each firm is only as strong as its weakest point.

We also asked firms if they used two factor authentication. This is recommended by Cyber Essentials:
[https://www.cyberessentials.ncsc.gov.uk/advice/]

> "For important accounts such as banking and IT administration, you should use two factor authentication, also known as 2FA. A common and effective example of this involves a code sent to your smartphone which you must enter in addition to your password."

This was routinely used by 25 firms for daily activities:

- 21 firms used it to enhance internal security, for example for remote workers and accessing information and/or software by staff
- 4 firms used it with clients to verify their identity and instructions during transactions.

Controlling access to systems and data

Significant damage can occur when software, hardware or data is misused or stolen. To mitigate this risk, firms should consider who has access to their system and the extent of the activities they allow. As Cyber Essentials outlines:

> "staff accounts should have just enough access to software, settings, online services and device connectivity functions for them to perform their role."

If a system is compromised, effective controls will also limit the amount of damage that can be achieved by criminals who have gained unauthorised access.

We were interested to find out more about:

- system access
- administration accounts
- physical security
- encryption.

We began by asking firms about the extent of access given to staff. Seven firms provided everyone with access to the entire system. This is significant because information may be misused or destroyed by accident. In addition, if intruders gained unauthorised access via a comprised log-in account, this would enable them to access all the firm's data.

We were also interested about the use of administration accounts. An administrative account should only be used to perform administrative tasks on a computer system, for example controlling the way the system works. If misused, administrative accounts can be used to install

malware and control the systems security settings so access to them should be limited to the smallest number of people necessary. To operate safely, firms should not allow staff to use administration accounts to carry out general work and fee earning.

We found 34 firms used accounts and permissions (including 15 firms who delegated administration duties to external IT companies). Two firms failed to use accounts and permissions. Four were unsure about their firm's arrangement.

It is important to monitor who has access to administration accounts:

- 21 firms kept a list of people who had access to administration accounts
- 16 firms monitored and reviewed the list
- 23 firms had systems in place to monitor staff activities on the system

This is particularly important where a firm's system can be accessed by an unauthorised device. This could include accessing the system through an online portal on a personal device. This is potentially vulnerable to a greater risk of unauthorised access. Significantly, 18 firms allowed such access and worryingly nine firms did not undertake monitoring of their systems to check who had accessed the system.

Firms should also consider the physical security of their systems and data. During each visit, we reviewed the physical security of each firm's servers and equipment. Most firms had taken steps to isolate and secure their servers. This included locking hardware away in specific cabinets/rooms and only allowing access to specific people. However, nine firms had noticeably poor security. This included:

- storing the server in the kitchen
- storing the server next to a window accessed by a fire-ladder.

These issues were often exacerbated because of the small and portable nature of the hardware.

We were also interested about the measures firms took to protect data and equipment if it was stolen:

- 50 percent of firms told us they had a system in place to track and delete data from laptops, tablets and phones remotely
- worryingly, 25 percent of firms told us that they did not encrypt their laptops.

Encryption is important because it converts information and data into a code and prevents third parties from reading it. Encryption helps to mitigate the extent of physical theft and cyber-attacks.

Protect yourself from malware and viruses

Malicious software (malware) is software designed to intentionally damage, control or effect hardware and software. It may also destroy, harvest or block access to data. There are many types of malware and they will often be operating without the system user's knowledge.

We asked firms basic questions about their knowledge of malware and the systems they use to combat malware. Thirty five firms were able to show us that they had active anti-virus software in place. Significantly, one firm had not turned the software on, and the remainder were unable to locate/check whether the software was active. A basic understanding of the anti-virus software and how it works is a necessity.

Malware can be downloaded online by accident via the internet or introduced into the system locally, for example by removable media such as data sticks (these were commonly used by 73% of firms). This might be done intentionally or by accident by cross contamination of different systems. Firms should consider how to monitor and mitigate the risks removable media poses. We found use of removable media was commonplace and often poorly monitored:

- 15 firms allowed fee earners to use their own data sticks
- 28 firms received data sticks from third parties such as estate agents or other solicitors
- 23 firms failed to monitor the use and provenance of data sticks.

If firms allow the use of data sticks, they should consider how they encourage and monitor safe usage.

Firms can also limit damage caused by viruses and malware such as ransomware by securing copies of their data, for example a backup. This enables information and software to be reloaded later to either the same system or a backup system. This is likely to be important where the firm is targeted by ransomware or other malware.

Each firm that we visited undertook some form of backup exercise.

This was an area where firms often relied on the assistance of third parties such as IT companies. During our review, seventeen firms told us that they couldn't access a copy of their last back up. Most firms stored data in multiple places:

- 31 firms stored data locally, for example within the firm
- 31 firms stored data remotely, for example in the cloud
- 22 firms did both.

Most firms created regular, automatic backups. Six firms took a manual back up. Firms who carry out manual backups should be careful to do so on a frequent and systematic basis. The effectiveness of a backup is

dependent on an ability to restore the system and data to a point in time. This may be hindered if there are significant gaps in the backup schedule. As outlined earlier, physical security of the hardware must also be considered.

Keep systems up to date

Cyber threats are constantly evolving. It is important that all software and hardware is routinely updated to make sure that systems are configured to reduce the effectiveness of known security vulnerabilities. All controls have a limited lifespan and once they have expired, they cease to be effective or useful. Significantly, updating devices and software is often simple and free.

A lack of knowledge about operating systems undermines a firm's ability to take sensible and necessary steps to protect itself and mitigate cyber risks.

We asked firms which operating systems they used:

Our findings raised some interesting points:

- Windows XP is no longer supported by Microsoft. Support and security updates for the software effectively ceased in 2014. Machines operating XP packages are likely to be vulnerable to cyber-attacks.
- At the time of our review, Windows 7 was due to stop receiving security updates and support in early 2020, so firms needed to consider whether additional hardware and software was required to update their system. Not all firms were aware of the impending January deadline.
- Windows 10 offers several security features. It can be configured to include multi-factor authentication, increased resilience to 'brute-force' attacks and automatic patching.

Patching should be carried out routinely and done as soon as the patch is released. A patch is provided by a software company when a security flaw is detected. Patching will occur throughout the lifetime of each piece of software and will improve its adequacy and effectiveness. We gathered information from firms about when patching occurred and who did it:

- 17 firms enabled automatic software patching
- 12 firms received patch support by an external specialist
- 4 firms told us they carried out patching as soon as required
- 7 firms told us they carried out patching on an ad-hoc basis.

A simple way to increase effective monitoring and updating is to understand the extent of a computer system. This can be done by creating a system inventory which logs each piece of hardware and software within the firm. Information can then be systematically checked to consider relevant updates and review potential vulnerabilities. Nineteen firms had put a system inventory in place.

Support

Aspects of cyber security are complex and technical. However, support is available and firms should use it.

> "It's rarely worth re-inventing the wheel. We don't advocate you blindly copying security solutions without any reflecting on how they fit your own context, but you can learn a lot from studying how other organisations have solved similar cyber security problems to yours ."[4 [#n4]]

We spoke to firms about whether they sought advice and support.

External IT companies

Thirty firms had arranged support from an external IT provider, with variable outcomes. We found that of these firms:

- 2 of the firms had a poor approach to cyber security
- 11 of the firms were poor in places.

The support and service provided by IT specialists varied from occasional, ad-hoc support to complete reliance. We consider complete reliance on a third party to be a risk that firms should avoid. During our visits we met two firms who had relied on specialists that were subsequently found to be providing a poor service. On both occasions, the experts' poor service had left the firms vulnerable. Both firms were subsequently forced to change their IT advisors and warned against the dangers of reliance and poor advice.

Insurance

Twelve firms had specific cybercrime insurance and eleven firms were investigating this area further. Beyond the provision of specific insurance cover, the twelve firms mentioned a range of other benefits:

- emergency contact information
- help with training
- help with analysing firm risk
- access to specialist advice and teams.

Significantly, firms told us that cyber insurance was often unavailable in the immediate aftermath of a cyber-attack because insurance firms perceived them as a higher risk.

Interest groups

Seven firms told us they were a part of a cyber security network or forum. These groups included:

- The Cyber Security Information Sharing Partnership – a joint industry and government initiative set up to share information and improve situational awareness.
- The International Legal Technology Association – an international body designed to support and connect people with peers within the legal sector.
- Two firms were involved in a local law enforcement scheme to share information and guidance about cybercrime.
- Two firms were part of bank/insurance led groups who provided support and advice to business leaders.
- One firm who was involved with their local law society cyber security group.

Firms said the groups offered positive and practical support.

Cyber Essentials Scheme

Cyber Essentials is a government backed scheme, that helps organisations take steps to protect themselves against common online threats. The scheme promotes basic technical controls that help businesses, regardless of their size and/or technical knowledge. The scheme requires organisations to adopt five technical controls:

- firewalls
- secure configuration
- user access control
- malware protection
- path management.

Organisations can either opt for a basic self-assessment option or apply for Cyber Essentials PLUS accreditation where systems and controls are audited by an external certifying body.

Our review found:

- five firms had Cyber Essentials Plus certification. Our review showed that these firms had a good approach to cyber security and we found they had implemented appropriate policies and controls
- sixteen firms told us they were working towards certification

- eighteen firms were not aware and/or interested in the scheme. Half of these firms had controls and/or processes that our review showed were either poor or poor in places.

Reporting

When issues occur, we expect firms and individuals to take appropriate steps and comply with their regulatory and legal reporting requirements[5] [#n5].

Reporting issues is significant. Not only is it a regulatory and statutory requirement, it also enables organisations to gather and share information. Firms also mentioned that they were provided with support and guidance by agencies once they made a report.

We were interested to find out more about when matters were reported by firms.

SRA

Information about successful cyber-attacks should be reported to us. Our Risk Outlook states: [/archive/risk/outlook/risk-outlook-2019-2020/]

> "Data breaches that might be serious breaches or misconduct should be reported to us through our Report Team. We are also interested in evidence of other cybercrime that affects firms and their clients. These can be sent to our Fraud Intelligence Unit"

We found:

- reports were not routinely made when clients were affected but the firm had not been directly involved, for example where clients were tricked to send money and information to a third party by e-mails purporting to be from firms. Although this is not a regulatory requirement the information would be helpful for understanding what is happening in the market and as part of raising awareness
- 29 firms had reported incidents to us
- seven significant incidents were not reported to us despite clear and significant breaches. This included five incidents of ransomware. Firms told us that they weren't sure whether we were interested in these issues. This is despite clear requirements to:
  - run their business effectively and in accordance with proper governance and risk management principles[6] [#n6]
  - protect client money and assets[7] [#n7].

Information Commissioner's Office

Certain cyber-crime incidents will need to be reported to the Information Commissioner's Office (ICO). Following a personal data breach, firms must make a report to the ICO within 72 hours[8 [#n8]] where they consider there is a risk to an individual's rights or freedoms[9 [#n9]].

The ICO defines a personal data breach [https://ico.org.uk/for-organisations/report-a-breach/] as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

Each breach must be assessed but not all breaches must be reported. However, it is likely that cybercrime incidents will lead to significant and serious breaches of personal data.

We spoke with firms about their ICO responsibilities:

- 9 firms had made a referral to the ICO following a cyber attack
- 9 firms encountered an incident where it appeared personal data had been accessed by an unauthorised individual, but no report had been made to the ICO. While this was historically not a mandatory requirement, it has always been considered best practice.

Law enforcement

Twenty three firms had informed law enforcement following their last cybercrime incident. On three occasions, firms hadn't contacted law enforcement despite serious incidents and substantial losses of client money:

- a client transferred £70K to a fraudster
- a further £70K transfer was made to a fraudster in an unrelated incident by another client
- a solicitor transferred £340K to a fraudster.

Underreporting is acknowledged by Action Fraud, the UK's national reporting centre for fraud and cybercrime:

> "On average, each police force in the UK recorded £19,626,323 in losses by businesses in their area. However, the true picture could be even higher, as these figures do not take into account the amount potentially lost by those businesses who choose not to report online crime to the police."

Appendix 1 - Methodology

Sample

During 2019, we visited 40 firms across England and Wales.

These firms were selected randomly from firms that had all been the subject of a report about cybercrime.

These firms ranged in size:

What we did

Each visit included interviews with two people at each firm. Initially, we spoke with individuals who had been nominated by the firm as their cyber security contact. We then interviewed a randomly selected member of staff.

Each interview included:

- questions about processes, systems and controls
- a review of the firm's policies and procedures
- interviewee perceptions
- a technical quiz.

Appendix 2 - Glossary

Antivirus software	Software that monitors systems and blocks cyber security threats.
Brute force attack	A cyber-attack using software to crack passwords by trial and error, inputting many combinations to gain access.
Cyber attack	Deliberate and malicious attempts to damage, disrupt or gain access to computer systems, networks or devices.
Cyber Essentials	A government-backed self-assessment certification that helps protect against cyber-attacks. It also demonstrates to others that a business is taking measures against cybercrime.
Cyber Incident	A breach of a system usually to gain malicious unauthorised access by a wide range of means.
Disaster Recovery Plan	An inventory of an organisation's hardware, software applications and data. It should include a contingency plan and a strategy to make sure that all critical information is backed up.
Email Modification Fraud	Criminals intercept and falsify emails between a client and their firm, leading to bank details being changed and money being lost

Encryption	The process of encoding information to make sure only authorised individuals can access it.
Firewall	A virtual boundary surrounding a network or device that is used to protect it from unwanted access. It can be hardware or software.
Hacker	Someone who breaks into computers, systems and networks.
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.
Government Communications Headquarters(GCHQ)	An organisation responsible for providing intelligence and information assurance to the government and armed forces.
Malware	Short for malicious software, it is used to disrupt computer operation, gather sensitive information or gain access to private computer systems.
National Cyber Security Centre (NCSC)	Part of GCHQ. A government organisation set up to help the public and private sector protect themselves against cyber-attacks.
Patching	The process of applying updates (patches) to hardware or software to improve security or enhance performance.
Phishing	A fraudulent attempt to obtain sensitive information from individuals. Techniques vary and include fake websites and e-mails. The techniques are generally untargeted. See also spear fishing.
Ransomware	Ransomware is a type of malware (malicious software) which encrypts all the data on a PC or mobile device, blocking the owner's access to it.
Spear phishing	A fraudulent attempt to obtain sensitive information from individuals by using a personalised message designed to look like it is from a person the recipient knows and trusts. See also email modification fraud.
Spoof email	An e-mail from a forged sender address.
Two-factor authentication	The use of two different components to verify a user's identity. Also known as multi-factor authentication.

Vishing	Phishing by voice. This 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.

Notes

1. Paragraph 5.2, SRA Code of Conduct for Firms 2019
2. Article 5(1)(f) of the General Data Protection Regulation (GDPR) 2016/679
3. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cybercrime [https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cybercrime]
4. https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/get-basics-right-risk-management-principles-cyber-security [https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/get-basics-right-risk-management-principles-cyber-security]
5. Paragraph 3.1 – 3.4, SRA Code of Conduct for Firms 2019 and Paragraph 7.1 – 7.6, 7.14 – 7.16, SRA Code of Conduct for Individuals 2019
6. Paragraph 2.1 – 2.6, SRA Code of Conduct for Firms 2019
7. Paragraph 5.2, SRA Code of Conduct for Firms 2019
8. Article 33 of the GDPR
9. Article 34 of the GDPR