Solicitors Regulation Authority

Risk Outlook report: information security and cybercrime in a new normal

1 June 2022

Executive summary

The move to remote and hybrid working has driven successful innovation from firms, as described in our latest report on innovation [https://qltt.sra.org.uk/sra/research-publications/risk-outlook-paper-innovation-competitive-landscape/] . It also means that they are more dependent on IT, so IT security is ever more important. Although the broad picture of information security and cybercrime threats have not greatly changed, it helps to be aware of how they are affecting the legal market.

The key types of IT threats we are seeing in reports to us are:

- Phishing and email modification frauds, which make up half of all the cybercrime reports we receive.
    - Although conveyancing remains a frequent target, due to the large funds involved, criminals are broadening their attacks to other fields as well.
    - Other sectors have been attacked using voice impersonation systems to copy a target.
- Ransomware, which is increasingly used to steal information and threaten to release it, can lock firms out of their own systems.
    - The loss of system access due to file encryption can seriously affect any firm, but especially those that are fully remote.
    - We are now receiving reports of cases where criminals have accessed sensitive client information, and it is likely that this will become the main type of ransomware attacks.
- Attacks on third parties and providers, which spread to solicitors' firms, is increasing
    - This has included compromises at an IT service provider and a barristers' chambers, both of which spread to multiple solicitors' firms.

Effective protection from these attacks means having the right culture, systems and training. We provide links to the most up to date advice in this report.

We want to continue to build our understanding about how these risks are directly affecting those we regulate. You can share your thoughts with us in our survey [https://form.sra.org.uk/s3/Risk-Outlook-2022] on how information security and cybercrime threats are affecting you, and how we, firms and the market can best respond to them.

Introduction

Covid-19 brought about greater use of IT. The post-pandemic 'new normal' will likely see that trend continue. However, as with most changes, this increased dependence on IT brings both opportunities and challenges. As well as creating opportunities and advantages for businesses and consumers, it also creates more opportunities for cybercriminals. And although we know firms have adapted to these threats and taken steps to defend themselves, cybercriminals continue to adapt too.

We know that, partly due to the requirements of lockdowns, more than half of surveyed solicitors [https://qltt.sra.org.uk/globalassets/documents/sra/research/full-report-technology-and-innovation-in-legal-services.pdf?version=4a1bfe] had improved or increased their use of existing technologies, and more than a third had introduced entirely new systems. Firms are increasingly taking advantage of automation, for example:

- embracing hybrid working [https://www.lawgazette.co.uk/news/firms-roll-out-flexible-office-return/5109766.article] with improved communications systems
- using online client contact systems such as chatbots [https://www.clio.com/blog/chatbots-for-lawyers/] or communication hubs
- experimenting with more advanced systems such as case analytics [https://emerj.com/ai-sector-overviews/ai-in-law-legal-practice-current-applications/] .

The majority of firms and their clients are using technology as part of their legal work. These developments have a very high potential to offer more effective, efficient, and more readily-available services.

While much of the picture of how information security threats are affecting firms has not greatly changed since our last update [https://qltt.sra.org.uk/sra/research-publications/risk-outlook-202122/] , we know that risks are still ever-present. We want to make sure that we have the clearest picture of how risks are affecting the market and how they might develop, so we can respond effectively to help firms meet the challenge now and in future.

In this report, we look at how the developing information security threats to firms could change in the near future. For a summary of the ways in which firms are benefiting from the opportunities that new working practices and technologies can bring, you will find the latest information in our accompanying Risk Outlook report on innovation [https://qltt.sra.org.uk/sra/research-publications/risk-outlook-paper-innovation-competitive-landscape/] .

Open all [#]

How are information security issues changing?

The fundamental challenge of how cybercrime threatens the data and information held by firms has not changed in the last few years. However, the reduced commercial activity in some areas during the lockdowns affected some types and levels of cybercrime.

The most significant threats, which we expect to remain the key areas, fall into three broad groups:

- phishing and email modification
- ransomware
- third-party attacks

Phishing and email modification

What do we already know?

Over 80 percent of all the cybercrime reports we received in 2021 involved email. It is very likely that many others, such as cases where firms were not certain how their systems had been compromised, had begun with a phishing email. This is because email is the easiest and most common type of attack, which provides a means of access for many types of cybercrime.

We are seeing an increase in email frauds that target a wider range of practice areas, in addition to conveyancing, where firms might be less alert to this threat. Another sign of adaptation comes from a report of criminals intercepting and falsifying physical mail between a firm and client to request funds.

How do we currently expect this to change?

We expect that cybercriminals will continue to seek easier targets. This could, in time, reduce the amount of money taken as the fields of law that deal with the most client funds become the most aware.

With firms focusing on the security of their IT systems, it is possible that criminals might make more use of false physical documents or voice-based phishing in the hope that their targets are less prepared.

There have been reports from other sectors that cloning a target's voice and mannerisms [https://www.bankinfosecurity.com/deepfakes-voice-impersonators-used-in-vishing-as-a-service-a-18050] has been used in phishing attacks. We have not yet heard of any cases where criminals have used voice-modification software in calls to impersonate a solicitor. With more work happening remotely, however, there is an increasing risk of firms becoming exposed to these sort of attacks. As they require access to recordings of a specific individual's voice, they cannot be used randomly or immediately.

However sophisticated the voice, and indeed video, impersonation systems become, they will be a threat only where criminals are targeting a specific individual with a very focused attack. Rather than phishing, the greatest threat from the use of these technologies might be the potential for impersonating jurors or witnesses in remotely heard legal cases.

Artificial intelligence (AI) is likely to play an increasing role in these threats, both positive and negative. Cyber security firms are making more use of these systems [https://gatefy.com/blog/how-ai-and-ml-fight-phishing/] in identifying phishing and malware. This is likely to play an increasing role in protecting against attacks.

However, criminals will also find uses for AI. The clearest use in the medium term will be making phishing contacts and other false communications more credible [https://red-goat.com/social-engineering/voice-cloning-heist] and harder to distinguish from the individual being copied. Such AI-assisted attacks have been very expensive to carry out in the past, but they are likely to become cheaper.

Case example: probate affected by email modification fraud

A solicitor was acting as co-executor of a client's estate. After an exchange of emails with their fellow executor, they authorised a substantial transfer of funds to what they had been told was the sole beneficiary's bank account. They received confirmation that the funds had been received.

A short time later, the other executor contacted the solicitor and asked whether they had received an order needed for the beneficiary. In discussing this, it became clear that the emails about funds had been from a criminal.

The firm investigated it and found that the perpetrator had started the email chain using the genuine address for the client. It appeared that either the firm, or the client's email system, had been hacked.

The firm took steps to remedy the matter. These included:

- moving money from their office account to the client account to cover the loss
- reporting the matter to their insurer
- commissioning a forensic investigation to find out whether their own accounts had been compromised

The firm also reported the matter to us – and we would urge all firms affected by cyber-attacks to do so - but we took no action as they had taken appropriate steps to remedy the matter, had told us promptly and it appeared to have been a one-off incident.

Ransomware

What do we already know?

Firms reported 18 ransomware attacks to us in 2021. This is not a large number, but attacks can have very serious impacts on firms. The cases that were reported to us may not give the true picture of the threat, as they represent only those cases where client information was affected. Older types of ransomware simply encrypted data, which meant that many attacks will not have involved a breach to report. Many attacks will not have affected client data beyond temporarily interrupting access to it, so although an attack can seriously harm a firm's ability to operate, not all attacks will have affected client data at all.

However, newer ransomware steals data as well as encrypting it, and threatens to release sensitive information as an additional pressure to get targets to pay the demanded ransom.

We have warned before that firms might come under attack with this newer, more dangerous form of ransomware. We are now receiving reports of firms encountering this.

How do we currently expect this to change?

This is clearly a growing threat. We expect that file stealing will become a normal part of how ransomware extorts money.

Ransomware will continue to increase in sophistication and to use a wider range of methods to influence its targets. It is likely to increasingly become fully automated [https://www.silverfort.com/blog/prevent-automated-propagation-of-ransomware-attacks/] , attacking any target with suitable weaknesses.

Most attacks will be random and be because the firm has a weakness that could be detected. However, some might be targeted intentionally. This could be used by unscrupulous parties to damage the operations of a firm that is acting for an opponent in litigation, for example. Those acting for clients operating nationally-significant infrastructure could be at higher risk of this in this time of international tension. The same applies to firms identified as acting [https://www.securityweek.com/cyberattacks-ukraine-new-worm-spreading-data-wiper-ransomware-smokescreen] for Ukrainian, Russian or Belarussian clients. There have been reports of cyberattacks used as a deniable weapon [https://www.reuters.com/article/us-ukraine-cyber-idUSKBN2AM1VF] and solicitors' firms might be seen, rightly or wrongly, as a less secure target than some of their clients.

With their dependence on IT infrastructure to operate, fully online firms and virtual networks could be particularly impacted by ransomware attacks. However, this type of threat could harm the operations of any firm.

Attacks on third parties

What do we already know?

There are many advantages to using more advanced IT and communications tools from third parties. We discuss these in the accompanying report on innovation [https://qltt.sra.org.uk/sra/research-publications/risk-outlook-paper-innovation-competitive-landscape/]. However, they also come with challenges.

We are increasingly seeing a trend of firms being affected by cyber-attacks on third parties. This can be direct, with criminals compromising the third party and attacking its customers with malware. It can also be indirect, where an attack on a provider harms the firm and its clients.

Examples we have seen include a compromised system at an IT service provider, which the criminals used to spread malware to the firm's customers and an attack on a barristers' chambers. Both of those spread to multiple solicitors' firms.

This trend could be a sign that firms are becoming harder targets, forcing the criminals to find indirect ways to attack. We have seen more cases of email modification fraud targeting intermediaries such as independent financial advisers, for example. And Action Fraud have noted a trend of criminals targeting the business clients of firms.

However, this trend also reflects firms' reliance on a wide range of third parties. In a remote-working world, IT infrastructure is more important than ever. That makes firms more dependent on their providers. Although many providers are likely to have stronger cybercrime defences, the dependence makes them more attractive targets for cybercriminals.

How do we currently expect this to change?

There are many ways in which firms' relationships with providers could expose them to attack. For example:

- virtual networks will be very dependent on their communications systems and therefore the risk of attacks is high for them
- cloud providers and other key IT systems can be compromised
- the spread of advanced IT tools, such as AI case analysis, from the largest firms to the remainder of the market. Firms will need to use an increasing range of services that in many cases will be remotely managed, but which require direct access to local data.

There are many ways that a compromised provider can be used to attack a law firm. At its simplest, it can mean sending phishing communications from the provider. One of the subtler methods is to modify a software

update [https://uk.pcmag.com/malware-protection-removal/132490/new-android-malware-poses-as-security-update-to-take-control-of-devices] to deliver malware.

AI systems might themselves in future be compromised by attackers seeking to alter their operations. This could create situations where the decisions and recommendations of an AI are altered to suit criminal ends. Firms might have a growing need to make sure that their provider can guarantee the integrity of their systems as well as their underlying accuracy.

Cybercriminals are also likely to make increasing efforts to attack smart contract systems. A system that automatically transfers money in response to defined trigger events will always be of interest to attackers. Many of these are based on blockchain systems that are, theoretically, verifiable. This means that they should be more secure [https://www.usenix.org/system/files/sec21summer_perez.pdf] against some frauds than traditional arrangements.

However, the fact that a contract's interpretation and enforcement are handled remotely on an IT system rather than personally by the parties creates chances to attack, even if those attacks have a low probability of succeeding. We can expect to see reports of attempted attacks emerging.

The ongoing move to provide more digital services in areas such as court judgments or land charges will create third parties that large numbers of solicitors will need to access. Although these services will be built to be secure, a successful compromise of one could cause widespread damage as well as potential wider harm to public confidence.

As well as causing disruption or using them to spread malware, criminals might try to alter information to gain advantage because more of the conveyancing system is moving online, and this is the most obvious future target. As an example, criminals seeking to carry out vendor frauds would benefit from the ability to alter ownership records.

It is therefore important to maintain the ability to verify known details about clients' legal situations.

Case example: firm affected by attack on IT provider

A firm was using an IT company to handle their network management. The ‘REvil' criminal group compromised the provider and used that control to distribute malware to users of its services.

The attack encrypted an older file system which held some client data. The firm's anti-malware defences detected the attack, and the firm promptly shut down all network access. This prevented the attackers from gaining further access to data.

The firm:

- reported the matter to us and to their insurers
- instructed a security specialist firm to help them make sure that none of their other systems were compromised
- did not attempt to access the encrypted drive, but deleted all corrupted files and restored operations from their secure backups.

We took no action against the firm, who had successfully defended against an attack from a normally trusted source.

What can your firm do?

Any firm holding money or confidential information is a potential target for theft. And any firm could be targeted with ransomware. As such, protecting clients' information must be a priority for all firms. Effective protection means having the right culture, systems and training.

Culture

The firms at most risk are those with cultures that do not encourage staff to come forward with problems. Everyone has times when they are distracted or stressed. At those times, people are more likely to fall for a phishing email, or to click on an attachment that they would otherwise have recognised as a scam. On those occasions, urgent internal reporting through your firm's IT security process is key to preventing more significant damage. This is because it could:

- entirely prevent some attacks aimed at subverting email accounts
- allow for at least some mitigation of ransomware attacks.

Firms can go a long way towards preventing the most frequent types of attacks by encouraging staff to report breaches immediately, and by building a no-blame culture. The tone set by senior staff is a crucial factor in this.

Systems

One of the simplest security measures involves choosing secure passwords, ideally backing them up with multiple-factor identification systems [https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661] . These systems do not guarantee that criminals cannot gain access, but they do make it harder. Our guidance section below gives links to current National Cyber Security Centre (NCSC) advice on how to choose effective passwords and secure access systems.

With face-to-face verification of identities less common in a remote working world, you will need to take additional care to make sure the

clients and third parties you are dealing with are who they say they are. This is not only an issue for information security, of course. Preventing money laundering, for example, also depends on effective identity verification.

As firms inevitably come to depend more on their IT providers and other third parties, it will be ever more important to establish that those providers can be trusted. Firms should take steps to protect their own systems against situations where a connected third party's systems have been compromised. This means taking steps such as having multiple backups, and having the ability to rapidly disconnect systems if an attack is detected. Firms should also familiarise themselves with how the provider will normally communicate and with how any software used will be updated.

You cannot directly defend your commercial partners from attacks. However, you can check that:

- you are dealing with businesses that are well reviewed and trusted
- you know your providers' service level guarantees in the event of service interruptions or data losses
- you know how quickly your provider is likely to recover in practice
- you know how your provider will prioritise service restoration among its clients.

You will not always be able to choose which third parties you and your providers are connected to, but care in choosing commercial partners will help to prevent some attacks.

Ultimately, however good your defences are, some attacks might make it through. We recognise this when investigating reports to us. As well as having recovery plans and backups, you could consider whether your specific needs require additional cyber insurance cover.

In building protective systems, it is important to make sure that they are proportionate and user-friendly. Systems that do not interfere too much with staff's ability to do their jobs are more likely to be used.

Training

If, like many firms, you are moving to hybrid working arrangements, you need to make sure staff remain aware of information security issues in the office, at home and on the move.

When staff have training on how to use their systems securely, for instance how to recognise the warning signs of phishing, then your firm will be in a better position to prevent attacks or will at least be better able to recover afterwards.

Where to go for further advice

Our cyber security Q&A [https://qltt.sra.org.uk/news/news/cyber-security-qa/] has information about how to minimise the risks of homeworking and remote meetings.

The NCSC [https://www.ncsc.gov.uk/] has advice and guidance for firms of all sizes. This includes:

- guidance on remote working [https://www.ncsc.gov.uk/guidance/home-working] , video meetings [https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations] and specific advice for smaller firms [https://www.ncsc.gov.uk/smallbusiness]
- guidance for businesses considering a 'bring your own device' [https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device] approach, and on how to safely use cloud services [https://www.ncsc.gov.uk/collection/cloud-security]
- advice on recognising and dealing with phishing scams [https://www.ncsc.gov.uk/guidance/suspicious-email-actions]
- advice on policies around the use of passwords [https://www.ncsc.gov.uk/collection/passwords/updating-your-approach] and other security systems
- free online elearning on defending against cybercrime and a free exercise [https://www.ncsc.gov.uk/information/exercise-in-a-box] to help firms test their resilience
- advice about new threats, such as criminal attacks on some cloud-based systems. [https://www.ncsc.gov.uk/news/rise-microsoft-office-365-compromise]

The British Standards Institution has advice about homeworking [https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2020/march/expert-advice-on-remote-working-from-bsis-cyber-security-and-information-resilience-team/] .

Cyber Essentials Plus [https://www.ncsc.gov.uk/cyberessentials/overview] is a government-supported scheme. It helps you assess your cyber security and has an external certifying body that audits your systems. Being certified under Cyber Essentials entitles some firms [https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/] to cyber liability insurance and technical help.

The ICO has guidance on your requirements under the General Data Protection Regulation (GDPR) and advice on how to protect you and consumers. And they have guidance on data protection and the coronavirus.

The Law Society's advice on cyber security for solicitors [https://www.lawsociety.org.uk/topics/cybersecurity/cybersecurity-for-solicitors] discusses how to protect your systems and comply with the GDPR.

Conclusions

One of the certainties about the ‘new normal’ is that information security threats will still be there. The underlying reasons why criminals try to hack legal firms have not changed. And in a legal market that is increasingly dependent on IT systems, criminals have more potential opportunities to attack using that method.

We will never have all of the answers. However, we will continue to give up-to-date advice and examples to help firms manage the risks while still gaining the benefits that technologies bring.

As we said in our previous Risk Outlook report [https://qltt.sra.org.uk/sra/research-publications/risk-outlook-202122/] , we want to build a better dialogue between ourselves and firms. This helps to build the best understanding and decision making, and lets us know how these risks are directly affecting those we regulate.

You can share your thoughts with us in our survey [https://form.sra.org.uk/s3/Risk-Outlook-2022] on how information security threats are affecting you, and how we, firms and the market can best respond to them.