National Cyber Security Centre
a part of GCHQ

Cyber Threat Report: UK Legal Sector

June 2023

Scope

The purpose of this report is to help law firms, lawyers and legal practices understand current cyber security threats, and the extent to which the legal sector is being targeted. It then offers practical guidance on how organisations can be resilient to these threats.

As the report explains, the cyber threat applies to law practices of all sizes and types of work, from sole practitioners, high street and mid-size firms to barristers' chambers, in-house legal departments and international corporate firms. Cyber criminals are not fussy about who they attack, which means small and large organisations are at risk.

The report has been compiled with the assistance of the NCSC's in-house cyber security experts, the NCSC-sponsored Industry 100 scheme, the Law Society, The Bar Council, the Solicitors Regulation Authority (SRA), Action Fraud (the UK's national fraud and cyber crime reporting centre) and the National Crime Agency (NCA). It has also drawn on an extensive body of open source reporting.

The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber security. Since the NCSC was created in 2016, as part of the Government's National Cyber Security Strategy, it has worked to make the UK the safest place to live and work online.

Contents

Foreword

Lindy Cameron - CEO NCSC

I am delighted to introduce the National Cyber Security Centre's (NCSC) Cyber threat report on the UK legal sector, an update to our first report published in 2018.

The legal sector is important to the NCSC as lawyers, legal practices and law firms play an essential role in the UK's economy and society. We rely on them for the delivery of justice, the resolution of disputes, and the conduct of business. This report will help ensure that the sector is as resilient as possible to cyber attack.

Organisations in the legal sector routinely handle large amounts of money and highly sensitive information, which makes them attractive targets for cyber criminals. Firms are vulnerable in new ways due to changing patterns of work – accelerated in the COVID-19 pandemic – and the increasing sophistication of cyber attacks. Recent examples affecting the legal sector have lead to a growing understanding of the problem at the highest levels of corporate governance, and the NCSC welcomes the increased support and investment in cyber security we're seeing across the sector.

Growing understanding of the issue at the highest levels of corporate governance, as well as great work from many professional legal bodies in supporting organisations and promoting improvements in cyber security practice, is all helping to improve the sector's resilience to the threat.

However, it is essential that scarce resources are focused in the right places to ensure that the risks to the legal sector from cyber attacks are effectively minimised. We hope this report will contribute towards that.

The Legal Sector Threat Report summarises the key issues facing the sector in 2023, supported by links to relevant NCSC guidance & services, designed to help lawyers and law firms maintain and improve their cyber security. We are committed to helping the sector stay one step ahead of the threat, so if you've any feedback on this report, or any suggestions for what more we can do to help, please don't hesitate to get in touch via the NCSC website.[1]

Malcolm Cree – CEO, The Bar Council

Individual barristers, chambers, and the Bar Council itself are increasingly reliant on the use of information technology to carry out essential daily functions and tasks to ensure the smooth operation of legal business.

Too many individuals and organisations have been the unfortunate victims of malicious cyber activity. This can include losing access to systems, theft, or deception. A cyber attack can cause absolute havoc, and it can impact staff, organisational processes, systems, finances, and reputations.

That is why this new report is both welcome and important. It provides extensive advice, information, and assistance to equip the legal sector with a better understanding of online threats. The report enables us all to reflect on the many challenges we face, and focus on building better cyber security resilience in the legal sector.

Lubna Shuja – President, The Law Society

This report is a timely and important resource for lawyers who wish to safeguard their systems and data against cyber threats.

Since the COVID-19 pandemic, the sector has drastically changed the way we work, which has led us to embrace a variety of new technologies. However, for all the positives that this change has brought, it also opens up new vulnerabilities to cyber attacks that can compromise our systems and the sensitive data we handle, leading to additional risks for firms.

The practical guidance and case studies included in this report will be very helpful for firms who want to increase their use of technologies, but in a safe and secure way. This in turn means that solicitors can continue to provide high-quality services for clients, while reassuring them that their data is secure.

By taking proactive steps to address cyber threats, we can continue to protect the rule of law, ensure access to justice, and provide secure legal services that allow businesses, individuals, and the wider economy to thrive.

The legal sector

The UK's legal sector is large and diverse, spanning organisations of many shapes and sizes, from small high street solicitors' firms to large multinational corporations, to self-employed barristers and barristers' chambers.

Legal services form an important component of the UK economy. As of early 2023, there were over 32,900 enterprises[1] in total including barristers, solicitors and other legal service providers operating in the UK, with an estimated total revenue of £43.9 billion[2]. More than 320,000 people work in the legal sector in the UK[3]. Legal services are an important export of the UK accounting for £6.8 billion of exports[4] as of 2021.

There is an inherent trust and strict confidence from clients that law firms preserve the confidentiality of their information. It is also a legal practice's overriding professional obligation, as set out in the professional standards, in the SRA's Standards and Regulations, the Bar Standards Board's handbook, and is common law, under the Legal Services Act 2007. It is essential that organisations maintain appropriate cyber security measures. Failure to do so can have exceptionally negative consequences for a legal practice and its clients.

The 2022 PriceWaterhouseCoopers Annual Law Firms Survey[5] reported that cyber risk has seen significant increases in spending among larger law firms, with the top 100 spending an average of 0.46% of fee income on cyber security in 2022.

Conventions used in this report

The legal sector includes businesses with very different structures and contexts:

- law firms range in size from large multinationals to small high street solicitors and sole practitioners
- barristers are often self-employed, but conduct their work through membership of chambers organisations
- many larger organisations have in-house legal departments for whom this report is also relevant

In this report, we use 'law firm' as a generic term, referring to all of these organisational arrangements. Where recommendations are more specific to a particular type or scale of organisation, we call this out in the text.

The UK's legal profession

- There are over 230,000 solicitors and legal executives practising in the UK.
- There are more than 18,000 barristers working in the UK, including around 700 sole practices, and the rest working out of the 400 chambers in the country.
- The legal sector includes many other specialists, including notaries, paralegals, will writers, immigration practitioners and licensed conveyancers.

The cyber threat

- Professional services, which includes the legal sector, is regularly at the top of analysts' leader-boards as the sector most impacted by the cyber threat.
- The Cyber Breaches Survey 2023[6] found that 32% of surveyed UK businesses identified cyber attacks.
- The SRA published 278 scam alerts in response to reports from the public and profession between January 2022 and January 2023. These scam alerts highlight reports of people falsely claiming to be solicitors and firms, for example on websites or in emails and telephone calls.

Why is the legal sector a particular target?

Entrusting law firms to safeguard highly confidential, commercially sensitive, and often personal information makes them prime targets for cyber criminals and other attackers. The results of accidental internal data breaches can be equally as challenging.

Law firms routinely handle highly sensitive client information (for instance relating to ongoing criminal cases, or mergers and acquisitions) that may be valuable to criminal organisations with an interest in exploiting opportunities for insider trading, gaining the upper hand in negotiations and litigation, or subverting the course of justice.

Disruption to routine business operations can be costly to legal practices, both in terms of billable hours lost due to outages and costs to clients that depend upon them, making legal practices particularly of interest to ransomware gangs aiming to extort money in return for restoration of IT services.

In many areas, from mergers and acquisitions to conveyancing, legal practices handle significant funds. The time pressures associated with transactions (as well as the large numbers of suppliers and clients and complex payrolls that law firms handle) create attractive conditions for phishing attacks and business email compromise.

Many legal practices, especially smaller firms, chambers and individual practitioners, rely on an external IT services provider, making it challenging for them to assess for themselves whether the controls they have in place are appropriate to the risk they face. A small law firm with few resources could be devastated if caught up by (for example) a ransomware attack. They are more vulnerable to attack, perhaps via unpatched vulnerabilities on unmanaged devices, or due to untrained staff or poorly offboarded leavers. Once attacked, a relatively small financial or reputational loss may be disastrous.

Reputation is critical to the business of law, which makes legal practices attractive targets for extortion.

Did you know?

- The SRA reported in 2020 that 75% of the solicitors' firms they visited for their cyber security thematic review[1] had been the target of a cyber attack in the past.
- The SRA[2] reports that 18 law firms were the victims of ransomware attacks in 2021.
- Nearly three-quarters of the UK's top-100 law firms have been affected by cyber attacks[3], and for smaller firms that have little or no dedicated cyber security and IT support, the risk of incidents like ransomware attacks is on the increase.

How things have changed since 2018

Since the release of the last Legal Sector Report in 2018, global events have affected the environment in which legal practices operate. In March 2020 after a wave of COVID-19 infections, many staff had to work remotely from home. This created challenges for maintaining secure working practices and protecting client confidentiality.

This shift to remote working has increased productivity across the legal sector[1], with most staff being happier and no longer having to commute. Working from home, they are able to concentrate and contemplate better. However, this shift can make collaboration and communication more difficult, which industries as a whole continue to grapple with.

The widespread uptake of remote working has increased risk from a cyber security perspective. Cyber criminals were quick to exploit concerns about the pandemic by creating COVID-19 related phishing emails[2] trying to trick users into clicking malicious links. Additionally, remote users were now connecting into their corporate networks from their home routers, which increased the risk exposure to the organisation's network.

The threat to the legal sector

In September 2020, the SRA produced a thematic review on cyber security[3] in the sector which highlighted how vulnerable the sector was, due to the large amounts of money that is handled between firms, their clients and other third parties. Significantly, out of the 40 law firms they visited, 30 reported they had been the target of a cyber attack. The remaining 10 firms reported that cyber criminals had directly targeted their clients during the course of their transactions.

In 2021, a city law firm reported that they had lost client data as a result of a cyber attack. It was reported that the market reacted swiftly, wiping off almost 8% share value within an hour of the statement. Additionally, the sector was subject to other attacks, this time targeting barristers chambers. This highlighted the importance of risk management when law firms engage barristers on client matters. The Law Society, Bar Council and members of the NCSC Industry 100 worked collaboratively to produce a risk-based questionnaire, which set out cyber security best practice.

More widely, we have seen an increase in 'cyber crime as a service'. Experienced attackers are increasingly selling their services to others, enabling even more criminals to target companies and individuals. They provide the products and the expertise to help novices deliver malware payloads or distributed denial of service (DDoS) as a service. In fact, cyber crime as a service is now so popular prices are being driven down by competition. This then increases the odds of being a victim, as more and more criminals have access to cyber skills.

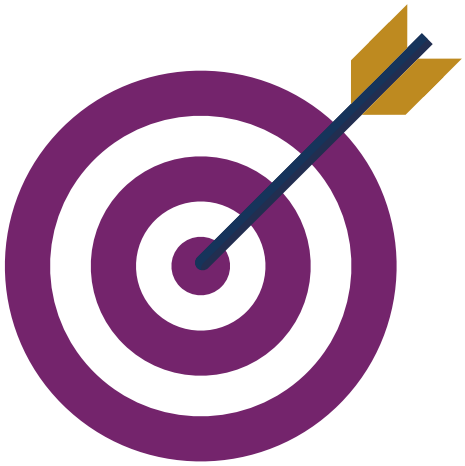
Defending hybrid working

The NCSC published guidance about preparing organisations (and staff) for home working[4], which included an infographic summary. The guidance contains advice on:

- Setting up user accounts and accesses.
- Helping your staff to prepare for home working.
- Controlling access to corporate systems through the use of VPNs.
- Helping staff to look after their devices, and to keep the software on them up to date.
- Using removable media safely.

Who might target the legal sector?

Like any other organisation, legal firms are increasingly reliant on IT. This section summarises the main individuals or groups that may target legal firms in order to steal funds, access sensitive information or conduct extortion. They may target your firm directly, or attack it through the suppliers you rely on. If necessary, they'll target your staff's personal devices as well as business equipment, networks and systems.



Cyber criminals

The primary threat to the UK legal sector stems from cyber criminals with a financial motive. Cyber criminals vary from advanced, professional groups to small-scale fraudsters. Criminals can buy 'off the shelf' services from more experienced cyber criminals, and so do not need advanced technical skills themselves. This change has led to an increase in the scale of cyber crime, with criminals indiscriminately attacking thousands of organisations - large *and* small - using predominantly automated tools that require little technical knowledge.

The NCSC are increasingly seeing 'hackers-for-hire' who earn money through commissions to carry out malicious cyber activities for third party clients, often involving the theft of information to gain the upper hand in business dealings or legal disputes. For their clients, they provide technical capabilities and deniability of involvement in the cyber attack were it to be discovered.

Nation states

Nation states conduct cyber activities to further their own national agenda and prosperity, or to disrupt professionals working on issues the state disagrees with, including human rights or those wanting regime change.

Russia, Iran and North Korea have all been identified as using criminal actors for state ends, operating to raise funds and cause disruption using criminal malware techniques. Major law firms are particularly exposed because they may be part of the wider supply chains used by nation states. The risk may also be greater for law firms that advise particularly sensitive clients, or work in locations that are hostile to the UK.

State actors, for example from China, have also used cyber techniques against UK institutions for intellectual property theft, which is a further risk for law firms dealing with intellectual property rights.

Hacktivists

Hacktivist is a term used to describe computer hackers motivated by a specific cause, for example to further political or personal agendas or in reaction to events or actions they perceive as unjust. Hacktivists have successfully used DDoS attacks to disrupt or deface websites.

The NCSC has observed some growth in the hacktivist community targeting law firms. The risk is greatest for those firms acting for organisations at odds with hacktivists' political, economical or ideological agenda, such as those that engage in work in the life sciences or energy sectors.

Insider threat

Insider threat is the deliberate or accidental threat to an organisation's security from someone who has *authorised* access such as an employee, volunteer, contractor or supplier. Despondent staff or ex-employees that hold a grudge, for instance, may have access to sensitive data and finances that can be exploited.

Insider threats are not always malicious. Employee breaches of security can stem from lack of staff training, or onerous processes which unwittingly encourage staff to 'cut corners' in order to get the job done. Or they can just be due to honest mistakes, such as clicking on a link in a convincing phishing attack. Managing staff security well is particularly vital in the legal sector, as many members of staff will have levels of access that are potentially of use to criminal groups.

The main types of cyber attack

Phishing

'Phishing' is when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make recipients visit a website, which will then download malware (such as ransomware or a virus) onto your computer, or steal bank details or other personal information (such as login details).

Phishing emails hide amongst the huge number of benign emails that busy users receive every day, and continue to be the most prevalent type of cyber attack against law firms. Given the ease with which millions of phishing emails can be sent at practically no cost, the majority are untargeted, often sent from free email accounts.

Most law firm websites contain vast amounts of information and contact details for their senior staff, partners and associates, which criminals can use (along with information from social and business networking sites) to launch more targeted attacks. One technique involves criminals monitoring LinkedIn to identify new joiners at an organisation, and then sending a scam email to the HR department. The scam emails contain a fraudulent request to change the payroll account details for the new joiner, in an attempt to steal salary payments.

Another common attack is to trick victims into disclosing their usernames and passwords. These phishing emails will often mimic Microsoft or Google login pages, and claim to relate to a fictitious legal matter that requires authentication to gain access. If the recipients enter their credentials, attackers can use these to conduct further attacks, or sell them on to other criminals.

Did you know?

The Cyber Breaches Survey 2023[5] reported that of the 48% of UK businesses who identified an attack, the most common threat vector was phishing attempts (79%).

Defending against phishing

The NCSC has produced specific guidance on defending your organisation against phishing attacks[1] which is suitable for medium to large-sized organisations. The guidance advises a multi-layered approach:

1. **Make it difficult for attackers to reach your users.** You can make it hard for attackers to spoof your email address by employing the anti-spoofing controls: DMARC, SPF and DKIM[2]. You should also carefully filter and block incoming phishing emails.

2. **Help users to identify and report suspected phishing emails.** Common features of phishing messages include urgency or authority cues that pressure the user to act. Try to create an environment that encourages users to report phishing attempts, adopting an approach of encouragement rather than punishment.

3. **Protect your organisation from the effects of undetected phishing emails.** It's not possible to stop all attacks. Malware is often hidden in phishing emails, or in websites that they link to. Well configured devices and good end point defences can stop malware installing, even if the email is clicked.

4. **Respond to incidents quickly.** Knowing about an incident sooner rather than later allows you to limit the harm it can cause. Incident response plans that cover phishing should be rehearsed before an incident occurs.

The NCSC has also produced phishing guidance for the following audiences:

- for small and medium sized organisations (which includes smaller legal firms): Avoiding Phishing Attacks[3]
- for individuals and families: How to spot a scam email, text message or call[4]

Business email compromise (BEC)

Business email compromise (or BEC) is a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information. Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals, and can be even harder to detect.

Law firms are attractive targets for BEC because they often transfer significant sums of money, or ask to view sensitive documents such as financial records, contracts and designs. They are also generally seen as trustworthy and authoritative, two qualities that attackers can make use of when devising a phishing attack.

During a BEC attack, criminals will either:

- use a **legitimate email account** that they've managed to access (for example, if an email is not protected by a strong password, or by multi-factor authentication)

or

- use a '**lookalike' email address**, that purports to be a real member of a legitimate company, but is in fact owned by the cyber criminal (for example, the email that you think is from john.smith@mycompany.com is actually from john.smith@myc0mpany.com)

A common tactic is to fabricate an email chain (or even more convincingly, duplicate a genuine exchange) with clients or suppliers relating to an invoice or payment. At an appropriate point, the attackers will send a doctored email with new bank details in an attempt to trick people into paying money into an account controlled by the attackers.

Malicious emails are also used as a platform to launch phishing campaigns against other law firms, as it is not unusual for multiple firms to be involved in a matter or case. Some emails may contain viruses disguised as harmless attachments, which are activated when opened.

Defending against business email compromise

- Use a takedown service[6] to monitor and assist with the removal of a domain that impersonates your organisation.
- Ensure that you implement SPF, DKIM and DMARC email protection for all your domains, even if they are not used for email.
- Ensure that it is easy for staff and external parties to report or query suspicious emails.
  Ensure that all important or unusual email requests are verified using another method (such as SMS message, a phone call, logging into an account, or confirmation by post or in-person).
- Ensure that strong and unique passwords are used for email accounts, and that they're additionally protected by multi-factor authentication (MFA). MFA should be enabled, where possible, for all critical business systems.
- Ensure that staff receive regular awareness training to help identify suspicious messages.

For further details, you can download the following infographic: Business email compromise: dealing with targeted phishing attacks (PDF)[7].

Crimson Kingsnake BEC Gang

In late 2022, reports[8] emerged that a new threat group called 'Crimson Kingsnake' were conducting large scale business email compromise (BEC) campaigns that were targeted at business customers of major law firms.

The group aimed to intercept transactions to acquire funds fraudulently by registering a large number of domains similar to major multinational law firms, and sent emails purporting to chase up payments for false invoices. This was an indiscriminate campaign and shows how the status of lawyers can be abused.

The emails use legal language to increase the sense of threat and urgency, and purport to be sent from - for instance, a 'Debt Collection Litigation Counsel' at a major international law firm. In some cases, these emails would be followed with a further reply impersonating a known senior individual from the victim organisation, asking that the bill be paid.

Ransomware and other malware

Ransomware is malicious software ('malware') that prevents you from accessing your computer, or the data stored on it. During a ransomware attack, your data is normally encrypted (so that you can't use it) or it may be stolen. The attackers may even threaten to publish your sensitive data online. This is a particular source of concern for the legal sector, which deals in highly sensitive information.

Attackers usually send a ransom note demanding payment to recover encrypted data, often using an anonymous email address. They will typically request payment in the form of a cryptocurrency. Furthermore, some criminal groups offer 'Ransomware as a Service' so that other malicious actors can commission attacks, putting the tools in the hands of any who are willing to pay.

The NCSC position, along with law enforcement, is that we don't endorse, promote or encourage the payment of ransoms. If you do pay the ransom:

- there is no guarantee that you will get access to your data or computer
- your computer will still be infected
- you will be paying criminal groups
- you're more likely to be targeted in future

We also encourage organisations to be open about ransomware attacks[9] by seeking support and communicating openly with the NCSC and Information Commissioner's Office (ICO). It can only help you, and will ultimately improve the threat landscape for everyone.

While ransomware receives a lot of attention in the media, it is important to have an awareness of other kinds of malware and to ensure that you have appropriate measures in place.

- **Adware** inserts malicious adverts into the user interface, for instance replacing legitimate adverts shown in a web browser.
- **Viruses, worms and trojans** are related forms of malware. Viruses are malicious code attached to legitimate executable files, while worms and trojans are standalone software, with trojans being designed to resemble a legitimate application.
- **Bots** are designed to interact with a system, and malicious bots may interfere with legitimate processes, or else provide command-and-control structures for a remote adversary (as in a 'botnet').
- **Keyloggers and spyware** are designed to run in the background on an infected device, and record user interactions, via peripherals such as webcams and keyboards, storing this data for exfiltration.

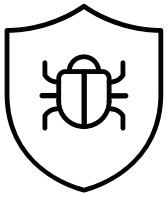
Tuckers Solicitors LLP

On 24 August 2020, a number of IT systems belonging to the criminal law firm Tuckers Solicitors LLP became unavailable, and upon investigation staff determined that they had been victim of a ransomware attack. Case data had been encrypted, as had backups. The attacker had also managed to exfiltrate data relating to 60 court cases, some of which were live, and published them on the dark web.

The root cause analysis was not conclusive, but it was deemed likely that the attacker gained access to Tuckers' systems by using a known system vulnerability. While this had been patched prior to the ransomware event, there had been a five month period between the release of the patch and its application to Tuckers' systems.

The ICO's decision to impose a fine[10] was based on the judgement of whether cyber security measures in operation at Tuckers were appropriate to the volume and sensitivity of the personal data being held. In justifying the fine, the Commissioner singled out, in particular, the absence of multi-factor authentication (MFA) on certain key systems, delays in the application of security patches, and the failure to encrypt stored personal data.

*Tuckers did **not** pay the ransom. In addition to fully co-operating with the ICO, Tuckers assisted the police on their investigation of the criminal group responsible for the hack and resolved all system issues to protect data going forward.*



Defending against ransomware and other malware

Steps you should take to defend against ransomware and other malware include:

- Make regular backups of your most important files, and check that you know how to restore files from the backup, and regularly test that it is working as expected. Ensure you create offline backups that are kept separate, in a different location (ideally offsite) from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment.
- Keep your software, and especially your operating systems, up to date. Set devices to 'auto-update', if you can, and apply security patches as soon as they become available.
- Carefully control what software and applications you choose to allow into your firm. You need to have some confidence in the provenance of software and ensure that is it suitably supported, which includes a mechanism for patching any security vulnerabilities.
- Use antivirus software to detect and isolate infected machines, and to scan backups to avoid reinfection.
- Implement strict controls over any means of remote access to your system.
- Draw up a plan for recovery and business continuity in the event of a ransomware attack or other incident, and rehearse the procedure to ensure it is well understood.

A more complete guide to defending against ransomware and other types of malware can be found in the NCSC's guidance on Mitigating malware and ransomware attacks[11].

Pegasus Spyware

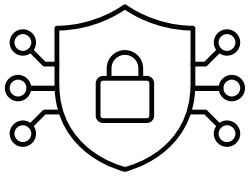
In 2021, it was reported[12] that lawyers - particularly those representing human right cases - were amongst those at risk of widespread use of commercial spyware, specifically the Pegasus software sold by Israeli-firm, NSO group. Pegasus is able to extract all of a mobile device's data and activate its microphone to listen in on conversations surreptitiously.

4 New Square

In 2021, Barristers Chambers 4 New Square were affected by a ransomware attack, which affected the operation of critical IT systems, and involved the exfiltration of sensitive data. As a result of the attack, their systems were briefly offline. However they were able to recover from their backups.

The investigation showed evidence of exfiltration and fortunately no publication took place. Cyber insurers mobilised a team shortly after the attack to isolate the systems, stop the attack and preserve the data. A significant GDPR data review exercise was subsequently carried out to ensure that proper notifications were made to any potentially affected clients.

The key lessons learned from this attack was that all plans should be tested. Although the response to the attack was successful and there was no significant disruption to clients in the immediate aftermath, had the plans in place been tested, recovery may have been quicker and smoother.



Password attacks

Access to data, systems and services need to be protected. Understanding who or what needs access, and under what conditions, is just as important as knowing who needs to be kept out. A good approach to identity and access management will make it hard for criminals to pretend they are legitimate, whilst keeping it as simple as possible for legitimate users to access what they need.

The core identity and access threats to law firms are:

Password re-use

Credentials are often re-used across multiple sites and services. This could allow a criminal to access work accounts if the password is disclosed, for instance in a data breach.

Weak passwords

Weak and common passwords are to easier crack, making it quicker for attackers to access law firm systems.

Excessive permission

By not restricting account permissions to data and services that are relevant, attackers have the opportunity to use compromised accounts to access more sensitive data and move onto other critical systems.

Open access

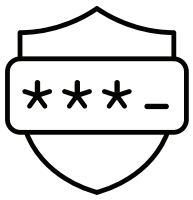
With the growing use of cloud systems to store confidential data, misconfiguration of these systems can leave data accessible to anyone. Attackers are very adept at searching across the internet to find these open access data sources.

MFA not enabled

Multi-factor authentication (MFA) adds an additional authentication step when logging into a system which makes it harder for an attacker to access systems, even if they have access to a valid account and password.

Defending against password attacks

- Ensure that your staff do not use the same credentials for logging into their work systems as they use for other services.
- Ensure all accounts are protected using strong passwords, and that staff are supported to understand how to do this (for example, by referring to the NCSC's guidance on using three random words[13])
- Staff will forget passwords, so make sure they can reset their own passwords easily.
- Restrict users' account permissions and data access to only those that are needed (a technique known as 'least privilege'). Regularly review access permissions, and ensure that your leavers process includes steps to promptly remove access.
- Implement MFA (or other types of authentication) for all accounts, where possible, so that you're not solely reliant on passwords. The NCSC's guidance 'Authentication methods: choosing the right type[14]' can help you decide what's right for your organisation.
- Change **all** default passwords before devices are distributed to staff. You should also regularly check devices (and software) specifically to detect unchanged default passwords.



Supply chain attacks

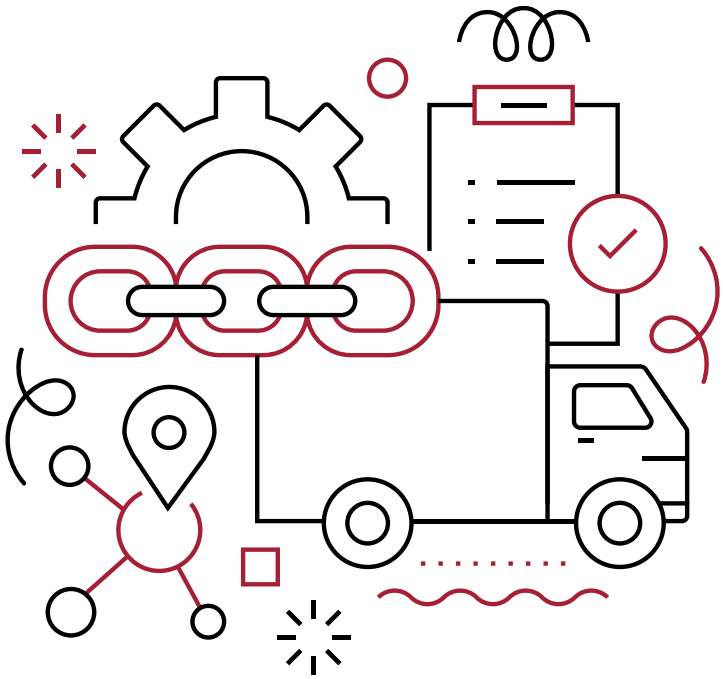
It is common, especially for smaller firms, to outsource the responsibilities for running, maintaining and securing their IT and data to specialist support companies. By far the greatest supply chain issue is a third party failing to adequately secure the systems that hold your sensitive data. Whilst you might be implementing cyber security effectively **within your own organisation**, you're exposed to numerous risks if your suppliers (or other third party in your supply chain) have not done the same.

Equally, cyber criminals may target **your** organisation in order to gain access to organisations that you do business with. A law firm's position in the global supply chain can also make them an attractive target for nation states, who have the resources and capabilities to gain access to corporate clients and their information.

The distributed nature of modern, complex supply chains increases the opportunities for criminals to conduct cyber attacks. Even for small to medium sized firms, suppliers will be wide and varied. This includes finance, billing and payments platforms, HVAC (heating, ventilation and air conditioning), and janitorial and cleaning systems.

Defending against supply chain attacks

- Understand your supply chain. Until you have a clear picture of your existing supply chain, it can make identifying risks and creating mitigation plans difficult. Ensure you have a list of all your suppliers, and partners, and identify which ones are highest priority. The NCSC's supply chain mapping training[15] can help you with this.
- Embed security within your contracting process. Build security considerations into your contracting decisions, and where appropriate require your suppliers do the same. The NCSC's supplier assurance questions[16] can help you gain confidence in your suppliers' cyber security.
- Larger organisations who need a more formal approach for assessing the cyber security of their organisation's supply chain should refer to the NCSC's supply chain guidance[17].



Reporting cyber attacks

The SRA has recently noted a decrease in the number of cyber security incidents being reported, and while this may reflect improvements in the sector as whole, it is concerning that there may be a reluctance to report as this can undermine sector-wide security efforts.

In the event of a ransomware attack or other cyber incident, organisations should:

- report an ongoing incident directly to Action Fraud[1] (on 0300 123 2040 which is available 24/7)
- for data breaches under the GDPR, report to the Information Commissioner's Office[2]
- for any major cyber incidents, report to the NCSC[3]

Reporting to the NCSC

All firms are strongly recommended to report incidents to the NCSC, the UK government's technical authority on cyber security.

The NCSC:

- provides support and incident response to mitigate harm
- works to ensure organisations have understood how they came to be a victim of a cyber attack
- ensures organisations have understood the cyber security implications (and taken steps to protect themselves from future attacks)

Sharing information on the cyber security issues you are facing enables the NCSC and professional bodies to analyse trends and issue relevant advice, and law firms in turn to invest their cyber security efforts in the right areas and to respond rapidly to emerging trends.

The NCSC is not a regulator and doesn't share information on incidents with the ICO, or any other regulators, without permission from the affected organisation.

Reporting to the Solicitors Regulation Authority

In England and Wales, the SRA's Code for Firms and individuals requires solicitors to report promptly to the SRA[4] any facts or matters they reasonably believe should be brought to their attention so that they may:

- investigate whether a serious breach of regulatory arrangements has occurred or
- exercise their regulatory powers

The SRA's guidance further recommends solicitors should report any cyber attack even if unsuccessful[5] or even if financial losses have been repaid.

If you discover that scammers are attempting to impersonate your law firm, for instance by creating a fake version of your website or impersonating your staff, you are encouraged to report this to the SRA[6] and the NCSC[7].

Simplify Group

In November 2021, the UK's largest conveyancing firm Simplify Group was the victim of a major cyber security attack that led to core business systems being taken offline. This resulted in a delay to completions, significantly reduced the number of new transactions and it was reported[8] to have cost the firm £6.8 million.

With a risk that personal data may have been accessed without authorisation, Simplify Group reported the incident to the Information Commissioner's Office (ICO), who said the group "fully complied with all relevant obligations required to ensure that data or information loss resulting from the attack was appropriately handled".

The incident demonstrated vividly to the sector the profound impact of business interruption on customers, and how a cyber incident should be reported to the relevant authorities.

How to improve your cyber security posture

We strongly recommend that all legal firms:

Ensure that senior leadership such as board members, owners and partners are engaged and informed about cyber security risk. The NCSC's Cyber Security Toolkit for Boards[1], provides a set of tailored resources to help senior stakeholders engage with these issues.

Assess your organisation against NCSC's Cyber Essentials[2]. This helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.

Sign up to the NCSC's key services that are available to help protect your organisation from a cyber attack. Services include Early Warning[3], Exercise in a Box[4] and Connect Information Share Protect (CISP)[5] .You may wish to consider Cyber Insurance[6], although this will not instantly solve all of your cyber security issues, nor will it prevent a cyber breach/attack.

Invest in staff training and awareness to improve the security culture in your organisation (see next page).

Cyber security training

Many large firms will have their own in-house training programmes, perhaps using content they've created themselves, or maybe buying in third-party training offerings. These should be regularly reviewed to ensure the content is keeping up with new threats. Use board member engagement to help drive training adoption across the organisation. In some cases, engaging an NCSC Certified Training provider[7] may be beneficial.

If you have no dedicated cyber security training in place, staff can work through the NCSC's e-learning package Top Tips for Staff[8], which is suitable for organisations of all sizes. It can be used in conjunction with existing policies and procedures, and can be modified to reflect your own branding and/or built into your own learning platform.

The importance of governance

Responsibility for cyber security ultimately resides at the top of an organisation, not with an IT supplier or department.

Different law firms have different structures and operate in different ways. Some firms are highly federated into individual practices, while others follow a more corporate structure. Partnerships, LLPs, sole practitioners, alternative business structures and incorporated firms will all have to develop governance arrangements that suit their context and risk.

Ultimately, it is the responsibility of the senior layer to ensure that cyber security is working effectively, and that means that those in a senior position must have adequate knowledge of cyber security to be able to make this judgement. The NCSC's Cyber Security Toolkit for Boards[9] is a set of resources designed to help seniors to do exactly this.

Membership services

There are a number of legal industry organisations that can be valuable to larger firms as a forum for information sharing.

- The International Legal Technology Association[10] has a dedicated group for security in legal ('LegalSec'), which focusses on sharing best practice.
- The Legal Services Information Sharing and Analysis Organisation (LS-ISAO)[11], is a threat intelligence sharing organisation with membership from United States, Canada, the United Kingdom and Australia.

CISP

The NCSC's Connect Inform Share Protect[12] (CISP) platform provides a secure forum where companies and government can collaborate on threat information. It is managed by the NCSC and membership is free. As a CISP member you can:

- access sensitive threat reports and the full breadth of NCSC advice
- share your own knowledge with other members on the platform, and also share new knowledge from CISP in your own organisation (where handling instructions allow)
- connect with other people in your sector or region, make new contacts and grow your network

Cyber security guidance

This section collates essential cyber security guidance and other useful documents for the legal sector.

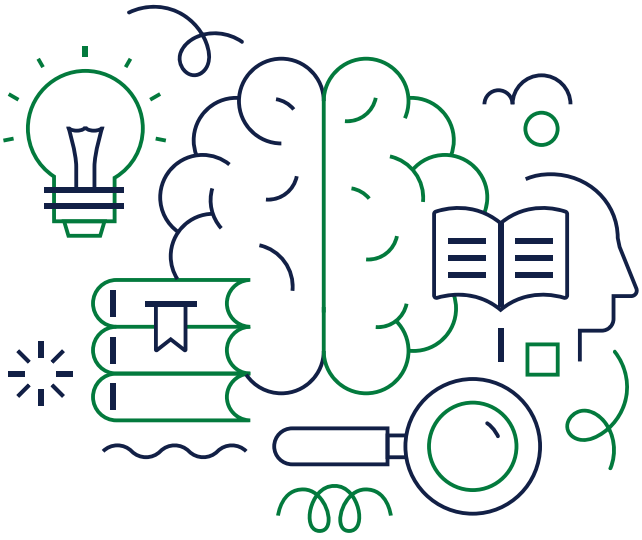
- Refer to the NCSC's guidance page[1] to browse our full list of cyber security publications.
- The Law Society also provides cyber security guidance for the legal sector[2] as does the International Bar Association[3].
- If your law firm's brand is being exploited online via a fake website, you can find out how to remove this in the NCSC's takedown guidance[4].

Guidance for sole practitioners and smaller practices

The NCSC's guidance for the self employed and sole traders [5] will be useful for sole practitioners.

The Bar Council provides guidance for barristers[6] on a wide range of cyber security topics, including on the application of GDPR to self-employed barristers[7].

The NCSC Small Business Guide[8] is ideal reading for smaller organisations working in the legal sector.



Medium to large practices

10 Steps to Cyber Security[9] is the NCSC's flagship guidance, and useful for all medium sized and larger firms. It's designed for security professionals and technical staff, and provides links to more detailed guidance where applicable.

The NCSC's Cyber Security Toolkit for Boards[10] helps senior managers to ensure that cyber resilience and risk management are embedded throughout their organisation, including its people, systems, processes and technologies.

Larger law firms with more complex IT can find out which areas to improve by applying for Cyber Essentials certification, or by running the Cyber Essentials readiness tool[11]. There are also other NCSC Products and Services[12] that will help to protect your organisation and reassure your customers that you take cyber security seriously.

The Bar Council Cybersecurity Questionnaire

The Bar Council have worked with the Law Society to produce a single common, standardised questionnaire, intended for solicitors' firms to review the information technology systems maintained by the chambers, and check if they're information security compliant.

This is because chambers often receive many different cyber security questionnaires from solicitors' firms, asking chambers to confirm that they have all their necessary cyber security measures in place. An agreed standardised solution eases the administrative burden on both the chambers responding to the questionnaire, and the law firms assessing those responses.

View and download the Cybersecurity questionnaire by the Law Society and Bar Council[13].

NCSC schemes and services

NCSC services

The NCSC provides a range of services, free at the point of use, to public sector and private organisations. They are delivered as part of the Active Cyber Defence programme[1], which aims to tackle the high-volume commodity cyber attacks that affect people's everyday lives.

The NCSC services of particular relevance to the legal sector include:

Early Warning[2]

Designed to inform your organisation of potential cyber attacks on your network, as soon as possible. The service uses a variety of information feeds from the NCSC, as well as trusted public, commercial and closed sources, which includes several privileged feeds which are not available elsewhere. Early Warning is open to all UK organisations who hold a static IP address or domain name.

Exercise in a Box[3]

An online tool which helps organisations find out how resilient they are to cyber attacks, and to practise their incident response in a safe environment. The service provides exercises, based around the main cyber threats, which your organisation can do in your own time as many times as you want. It includes everything you need for setting up, planning, delivery, and post-exercise activity.

Check Your Cyber Security[4]

This is a free government service, suitable for smaller firms, that performs a range of simple online checks to identify common vulnerabilities in your public-facing IT. All checks are remote, without the need to install software and it uses the same kind of publicly available information as cyber criminals use to find easy targets.

Cyber Essentials Scheme

The NCSC's Cyber Essentials scheme[5] ,provided through the IASME Consortium, assesses organisations' ability to protect themselves from the most common cyber threats, and reassures their stakeholders that cyber security is taken seriously. All practices qualified under the Law Society's Lexel[6] Legal Practice Quality Mark should be accredited against Cyber Essentials.

UK organisations with a turnover under £20m that achieve whole-organisation Cyber Essentials certification are eligible for free Cyber Liability Insurance[7].

As well as paid certification routes, IASME runs a free Cyber Essentials readiness tool[8] that will create a personal action plan to help you move towards meeting the Cyber Essentials requirements.

All links

Foreword
[1] https://www.ncsc.gov.uk/contact

The legal sector
[1] https://www.nomisweb.co.uk/datasets/idbrent
[2] https://www.ons.gov.uk/economy/economicoutputandproductivity/output/datasets/monthlybusinesssurveymbsturnoverofservicesindustries
[3] https://www.barstandardsboard.org.uk/news-publications/research-and-statistics/statistics-about-the-bar/practising-barristers.html
[4]https://www.ons.gov.uk/economy/economicoutputandproductivity/output/datasets/monthlybusinesssurveymbsturnoverofservicesindustries
[5] https://www.pwc.co.uk/industries/legal-professional-business-support-services/law-firms-survey.html
[6] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Why is the legal sector particularly a target?
[1] https://www.sra.org.uk/sra/research-publications/cyber-security/
[2] https://www.sra.org.uk/sra/research-publications/risk-outlook-report-information-security-cybercrime/
[3] https://www.legalfutures.co.uk/blog/is-your-law-firm-protected-from-ransomware-attacks

How the cyber threat has changed since 2018
[1] https://www.legalfutures.co.uk/associate-news/the-future-of-work-what-hybrid-means-for-the-legal-industry
[2] https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus
[3] https://www.sra.org.uk/sra/research-publications/cyber-security/
[4] https://www.ncsc.gov.uk/guidance/home-working

Who might target the legal sector?
[1] https://www.thebureauinvestigates.com/stories/2022-11-05/inside-the-global-hack-for-hire-industry

The main types of cyber attack
[1] http://www.ncsc.gov.uk/phishing
[2] https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing
[3] https://www.ncsc.gov.uk/collection/small-business-guide/avoiding-phishing-attacks
[4] https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams
[5] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
[6] https://www.ncsc.gov.uk/guidance/takedown-removing-malicious-content-to-protect-your-brand
[7] https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf
[8] https://www.theregister.com/2022/11/04/crimson_kingsnake_bec_scam/
[9] https://www.ncsc.gov.uk/blog-post/why-more-transparency-around-cyber-attacks-is-a-good-thing-for-everyone
[10] https://www.legalfutures.co.uk/latest-news/top-criminal-law-firm-fined-98000-for-cyber-security-negligence
[11] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
[12] https://www.theguardian.com/news/2021/jul/19/spyware-leak-suggests-lawyers-and-activists-at-risk-across-globe
[13] https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
[14] https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type
[15] https://www.ncsc.gov.uk/guidance/mapping-your-supply-chain#section_6
[16] https://www.ncsc.gov.uk/guidance/supplier-assurance-questions
[17] https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security

Reporting cyber attacks

[1] https://www.actionfraud.police.uk/
[2] https://ico.org.uk/for-organisations/report-a-breach/
[3] https://report.ncsc.gov.uk/
[4] https://www.sra.org.uk/solicitors/guidance/reporting-notification-obligations/
[5] https://www.sra.org.uk/sra/research-publications/risk-outlook-2020-21/information-and-cyber-security/#:~:text=Certain%20cybercrime%20incidents%20involving%20personal,breach%20of%20our%20Accounts%20Rules.
[6] https://www.sra.org.uk/consumers/problems/fraud-dishonesty/scams/
[7] https://www.ncsc.gov.uk/section/about-this-website/report-scam-website
[8] https://www.legalfutures.co.uk/latest-news/cyber-attack-cost-conveyancing-giant-7m-plus-lost-business

How to improve your cyber security

[1] https://www.ncsc.gov.uk/collection/board-toolkit
[2] https://www.ncsc.gov.uk/cyberessentials/overview
[3] https://www.ncsc.gov.uk/information/early-warning-service
[4] https://www.ncsc.gov.uk/information/exercise-in-a-box
[5] https://www.ncsc.gov.uk/cisp/home
[6] https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance
[7] https://www.ncsc.gov.uk/section/products-services/ncsc-certification
[8] https://www.ncsc.gov.uk/training/v4/Top+tips/Web+package/content/index.html#/
[9] https://www.ncsc.gov.uk/collection/board-toolkit
[10] https://iltanet.org/
[11] https://www.ls-isao.com/
[12] https://www.ncsc.gov.uk/cisp/home

Cyber security guidance

[1] https://www.ncsc.gov.uk/section/advice-guidance/all-topics
[2] https://www.lawsociety.org.uk/topics/cybersecurity/
[3] https://www.ibanet.org/LPRU/Cybersecurity
[4] https://www.ncsc.gov.uk/information/takedown-service
[5] https://www.ncsc.gov.uk/section/information-for/self-employed-sole-traders
[6] https://www.barcouncilethics.co.uk/subject/it/
[7] https://www.barcouncilethics.co.uk/documents/gdpr-guide-barristers-chambers/
[8] https://www.ncsc.gov.uk/collection/small-business-guide
[9] https://www.ncsc.gov.uk/collection/10-steps
[10] https://www.ncsc.gov.uk/collection/board-toolkit
[11] https://getreadyforcyberessentials.iasme.co.uk/
[12] https://www.ncsc.gov.uk/section/products-services/introduction
[13] https://www.barcouncil.org.uk/resource/cyber-questionnaire-by-the-law-society-and-bar-council.html

NCSC schemes and services

[1] https://www.ncsc.gov.uk/section/active-cyber-defence/introduction
[2] https://www.ncsc.gov.uk/information/early-warning-service
[3] https://www.ncsc.gov.uk/information/exercise-in-a-box
[4] https://checkcybersecurity.service.ncsc.gov.uk/
[5] https://www.ncsc.gov.uk/cyberessentials/overview
[6] https://www.lawsociety.org.uk/topics/firm-accreditations/lexcel/
[7] https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/
[8] https://getreadyforcyberessentials.iasme.co.uk/questions/

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C113965