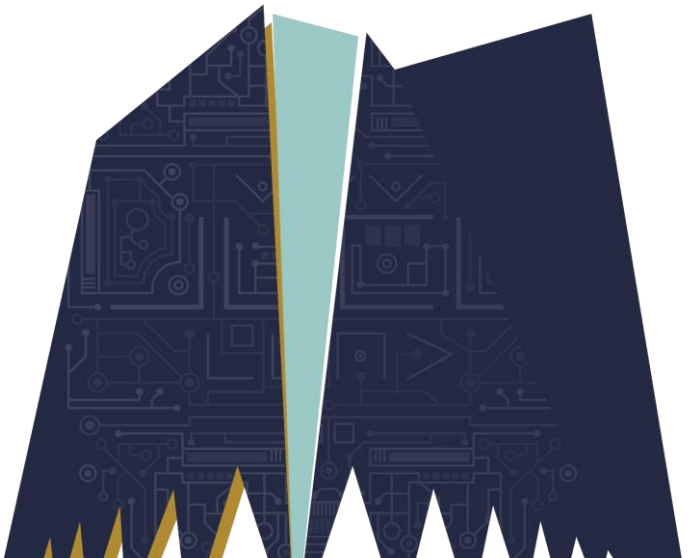
National Cyber Security Centre
a part of GCHQ

The Law Society

National Cyber Security Centre
INDUSTRY 100

The cyber threat to UK legal sector

2018 Report



Contents

Scope of the report

The purpose of this report is to help law firms understand current cyber security threats and the extent to which the legal sector is being targeted. It also offers practical guidance on how they can protect their practice. The cyber threat applies to law firms of all sizes and practice, from sole practitioners, high street and mid-size firms, in-house legal departments up to international corporate firms.

The report has been produced in direct response to a requirement from the legal sector and forms part of the NCSC's mission to raise the cyber maturity and resilience of law firms. It is intended to engage senior decision makers in the legal sector and encourage industry-wide adoption of cyber security best practice.

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 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 report provides an overview of the most significant cyber security threats to law firms, including a case study on the impact and guidance on mitigations. It also contains guidance on how to report a cyber attack and to whom (see Annex A).

"Like all businesses, law firms are increasingly reliant on IT and technology and are falling victim to a range of malicious cyber activity. Losing access to this technology, having funds stolen or suffering a data breach through a cyber attack can be devastating, both financially and reputationally, not only for the firm but also their clients. The NCSC is not just here to look after the IT systems of UK government. We are committed to supporting the legal sector and we encourage you all to implement the guidance outlined in this report."

Ciaran Martin - Chief Executive Officer, NCSC

"As data controllers, law firms handle significant volumes of confidential and sensitive information and client monies as part of their daily work. In the post-GDPR world and as the sector delivers and transacts more online, it's vital that we get a common view and understanding of cyber threats and their impact. The Law Society sees this report as a positive step to help our members spot vulnerabilities and put relevant safeguards and protections in place."

Christina Blacklaws - President, The Law Society

National Cyber Security Centre
INDUSTRY 100

"Improving cyber security across the legal sector is critical for the future of our practice. Through the Industry 100 scheme, the legal community has built a strong partnership with NCSC to develop and share relevant, actionable information that will have a real impact across our sector."

Industry 100 Law Firm Partners

Executive summary

- In common with many other industries, the cyber threat to the UK legal sector is significant and the number of reported incidents has grown substantially over the last few years. According to the 2017 PricewaterhouseCoopers Law Firm survey, 60% of law firms reported an information security incident in the last year, up from 42% in 2014[1].

- The financial and reputational impact of cyber attacks on law firms is also significant. The costs arise from the attack itself, the remediation and repairing reputational damage by regaining public trust. The SRA reports that over £11 million of client money was stolen due to cyber crime in 2016-17[2] .

- There are several factors that make law firms an attractive target for cyber attack – they hold sensitive client information, handle significant funds and are a key enabler in commercial and business transactions. The risk may be greater for law firms that advise particularly sensitive clients or work in locations that are hostile to the UK. For example, firms acting for organisations that engage in work of a controversial nature such as Life Sciences or the energy sector may also be targeted by groups with a political or ideological agenda. The move to offer legal services digitally will not only provide new opportunities but also further avenues for malicious cyber exploitation.

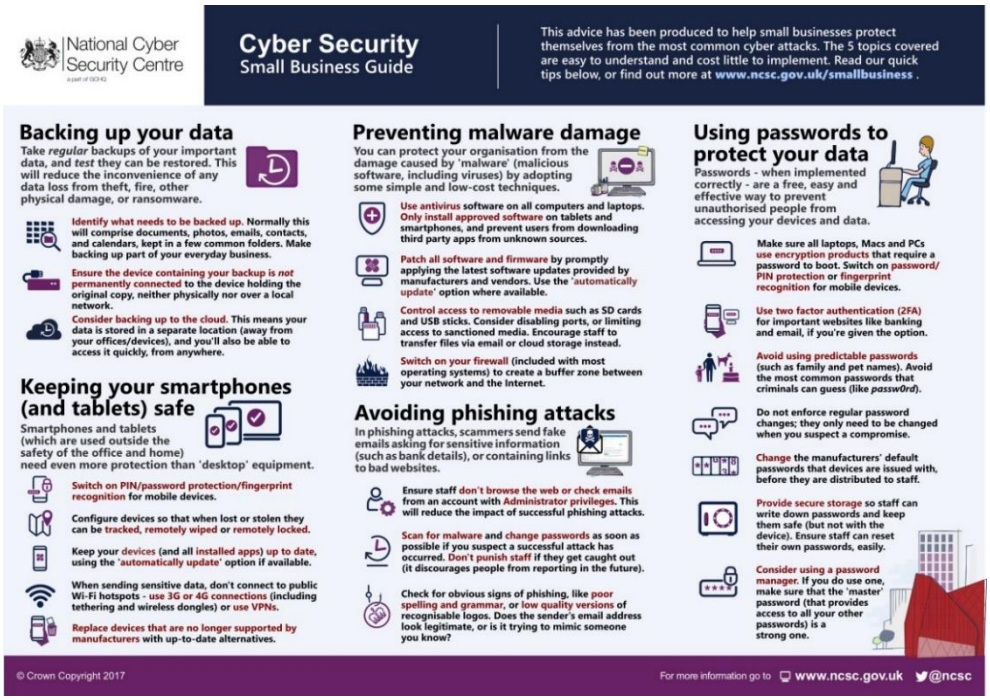
- The primary threat to the UK legal sector stems from cyber criminals with a financial motive. However, nation states are likely to play an increasingly significant role in cyber attacks at a global level, to gain strategic and economic advantage . There has also been some growth in the hacktivist community targeting law firms to achieve political, economic or ideological ends.

- The most significant cyber threats that law firms should be aware of are:
    1. Phishing
    2. Data breaches
    3. Ransomware
    4. Supply chain compromise

[1] https://www.pwc.co.uk/industries/law-firms/law-firms-survey-report-2017.pdf
[2] https://www.sra.org.uk/sra/news/press/risk-outlook-2017.page

- Cyber security is all too often thought of as IT issue, rather than the strategic risk management issue it actually is. If you don't protect highly sensitive client information, your whole practice may be in jeopardy. The NCSC's 10 Steps to Cyber Security[3] is a guide to help board members ask the right questions of their firm about cyber.

- For straightforward technical tips to work on immediately, law firms are encouraged to follow the NCSC's Small Business Guide[4]. This is particularly useful for smaller firms with limited resources. See Annex B for technical, policy and awareness actions that are included with this guidance.



[3] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

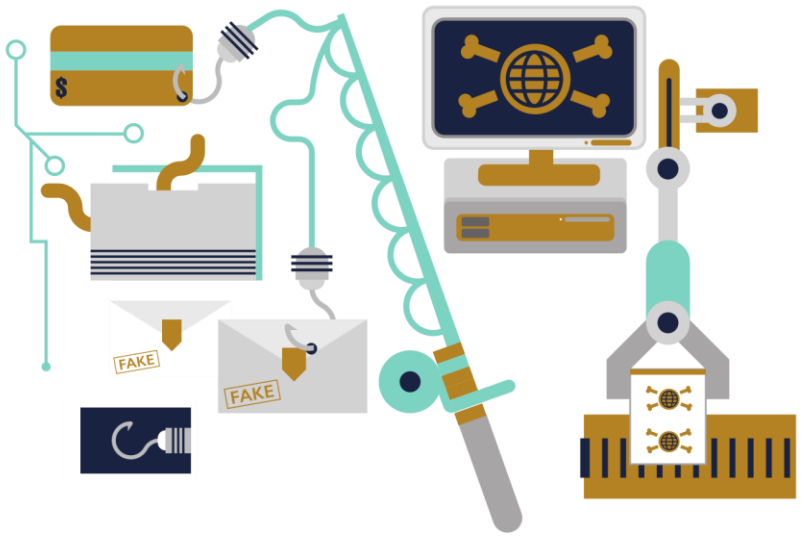
[4] https://www.ncsc.gov.uk/smallbusiness

Cyber threats to the legal sector

Cyber threats to the legal sector come in various forms, the most significant of which are described in this section. The threat actors are primarily cyber criminals with a financial motive, however there has been some growth in nation state actors[5] and the hacktivist community targeting overseas-based law firms to achieve political, economic or ideological ends[6].

1. Phishing

Phishing describes a type of social engineering where attackers influence users to do 'the wrong thing', such as disclosing information or clicking a bad link. Phishing can be conducted via a text message, social media or by phone, but most people use the term 'phishing' to describe attacks that arrive by email. Email is an ideal delivery method for phishing attacks as it can reach users directly and hide amongst the huge number of benign emails that busy users receive[7]. Phishing can target both law firms and their clients, with cyber actors spoofing a firm's email address to make messages to clients more convincing.



The amount stolen from law firms through phishing in the first quarter of 2017 was 300% higher than the previous year[8].

Phishing is the most common cyber attack affecting law firms and is particularly prevalent in areas of practice such as conveyancing. A recent poll of law firms showed that approximately 80% have reported phishing attempts in the last year[9]. Its relative low cost/low tech - high reward relationship makes it a popular and lucrative method for cyber criminals. The amount stolen from law firms through phishing in the first quarter of 2017 was 300% higher than the previous year.

[5] https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html
[6] https://www.dowjones.com/insights/rising-hacktivist-attacks-take-companies-surprise/
[7] https://www.ncsc.gov.uk/phishing#what
[8] https://www.sra.org.uk/sra/news/press/risk-outlook-2017.page
[9] Law Society research: online cybersecurity poll, June 2018 and i100 partners

The SRA website details 110 scams against law firms so far in 2018[10] . These are the known scams, there are likely to be many more that go unreported. One of NCSC Industry 100 partners[11] estimate that they receive over 11,500 phishing emails every month, across 5,000 staff.

Case study: phishing attack on mid-sized law firm with multi-million pound turnover

A senior partner broadcast on social media full details about a business trip to Barcelona (flight, meeting plans, weather etc). A criminal gang based overseas used this information to initiate a phishing attack against the firm's accounts team.

An accounts clerk received an email from an account spoofing the senior partner's email address, instructing her to pay an invoice and imploring confidentiality. Even though the firm had in place a number of policies and procedures that systemised the payment of invoices, they were able to persuade the accounts team to bend the rules, under the pretext of urgency, confidentiality and seniority.

The criminals also knew that the accounts team were tied up in installing a new accounting package and training on the new system, as a staff member had mentioned it on Facebook.

It was at this time that the criminals convinced the clerk to make an authorised payment of £35,000. The firm only realised it had fallen victim to phishing when another senior partner later queried the transaction.

In response, the firm reviewed every aspect of the business, including how staff interact with senior partners and how they ensure compliance with internal procedures. It also changed its social media policy.

When the firm was subject to a subsequent phishing attack worth £100,000, it successfully defended itself.

Mitigations against phishing

In addition to the 10 Steps and Small Business Guide, the NCSC has produced some specific guidance on defending your organisation against phishing. NCSC advises a multi-layered approach:

1. Make it difficult for attackers to reach your users.
2. Help users identify and report suspected phishing emails.
3. Protect your organisation from the effects of undetected phishing emails.
4. Respond quickly to incidents.

Further details can be found here:

- www.ncsc.gov.uk/phishing
- www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing

[10] https://www.sra.org.uk/consumers/scam-alerts/scam-alerts.page

[11] https://www.ncsc.gov.uk/information/industry-100

In addition to the above, law firms should ensure that their business processes are robust against phishing, for example:

- Implementing processes to verify (via independent means) invoices and account details for money transfers.
- Using 'cooling off' periods for changing account details for high value transactions.
- Encouraging a culture where suspicious transactions are queried and rushed or improperly validated payments are refused.
- Educating your clients about your firm's invoice and money transfer processes to help them avoid falling victim to a phishing attack.

2. Data breaches

The loss of client information can have a devastating impact on a sector that has confidentiality at the heart of its business. Law firms with politically or commercially sensitive clients are likely to be at a higher risk of data breach than a local high street firm.

Mossack Fonseca lost the largest amount of data ever recorded (2.6tb)[12]. The damage to the firm's reputation meant it never recovered and had to close.

According to Action Fraud, in the two years to March 2018, eighteen law firms reported hacking attempts. Such attacks tend to be more targeted in nature and are most likely initiated by phishing. They are often the work of more sophisticated cyber actors such as organised crime groups and nation states.

For example, three foreign nationals successfully infiltrated the networks of two New York-based law firms to steal inside information (about pending mergers and acquisitions deals) and trade on it. The unlawful gains exceeded $4 million[13]. Iranian hackers for hire have also reportedly targeted law firms (amongst other private sector companies) to obtain Intellectual Property to sell on to Iranian government entities.[14]

[12] https://www.scmagazineuk.com/updated-panama-papers-who-let-the-docs-out/article/531685/

[13] https://www.forbes.com/sites/roncheng/2017/01/11/china-based-hacking-case-against-u-s-ma-firms-illustrates-cyber-security-and-enforcement-issues/#10bd29b23c58

[14] https://threatpost.com/fbi-iranian-firm-stole-data-in-massive-spear-phishing-campaign/130776/

Law firms should also be aware of the insider threat – both accidental and malicious. The latter may come from an employee seeking financial gain or with a perceived grievance against the firm. According to The Industry Security Forum, over half of all data breaches are caused by insiders[15].

Case study: Mossack Fonseca data breach[16]

In 2016, Panama based law firm Mossack Fonseca suffered a major data breach commonly known as the Panama Papers hack . It lost the largest amount of data - 2.6 TB - ever recorded.

The blow to the firm's reputation meant it never recovered and had to close. The breach was believed to have occurred because the firm's client portal had not been updated since 2013. The portal contained several security weaknesses.

The motivation behind this leak and the 2017 leak (1.4 TB) of the Paradise Papers from an offshore law firm (by as-yet unidentified hackers) was reportedly to expose supposed global elite wrongdoing.

Mitigations against data breaches

In addition to the 10 Steps and Small Business Guide, the NCSC and the Information Commissioner's Office (ICO) have produced some specific guidance on what they consider to be appropriate measures under the General Data Protection Regulation (GDPR):

1. Manage security risks to personal data.
2. Protect personal data against cyber attack.
3. Detect potential security incidents and monitor user access.
4. Minimise the impact.

Further details can be found below:

- https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The Centre for the Protection of National Infrastructure (CPNI) also offers guidance on reducing insider risk from a personnel security perspective: https://www.cpni.gov.uk/reducing-insider-risk

[15] https://www.securityforum.org/research/managing-the-insf-briefing-paper/

[16] https://www.theguardian.com/world/2018/mar/14/mossack-fonseca-shut-down-panama-papers

3. Ransomware

Ransomware is a type of malware that prevents the victim from accessing files or data on their computer or network until a ransom has been paid[17]. Paying the ransom does not guarantee that you will get access to your data/device, and attackers may assume that you would be open to paying ransoms in the future[18].

A screenshot of a computer infected with NotPetya. The attack illustrates vividly what can happen to a firm subject to a ransomware attack, whether specifically targeted or not.

High-profile cyber crime incidents such as WannaCry in May 2017, which affected 200,000 computers in 24 hours, highlight the indiscriminate nature of such attacks. Email is the most common attack vector for ransomware: a recent estimate is that 80-90% of ransomware attacks come via this method[19].

Ransomware is designed to cause widespread business disruption. Whilst a law firm may not be the intended target of a ransomware attack, they may well suffer collateral damage, depending on the methodology used. The NotPetya attack illustrates vividly what can happen to a firm subject to a ransomware attack, whether specifically targeted or not.

[17] http://www.lawyersdefencegroup.org.uk/ransomware/

[18] https://www.ncsc.gov.uk/guidance/mitigating-malware#what

[19] https://www.newstatesman.com/spotlight/2018/05/fortifying-castle-walls

Case study: DLA Piper NotPetya[20]

In 2017 DLA Piper suffered a global ransomware attack that caused significant business disruption for a number of weeks. It is to date the single biggest cyber attack to ever hit any law firm and it affected almost the entire IT infrastructure.

The attack utilised a new variant of the Petya malware (NotPetya) via the software update mechanism of M.E. Doc, a Ukrainian tax program, that had been compromised to spread the malware. The attack appeared to be a ransomware attack; it was later identified as a destructive variant so that the data was encrypted.

DLA Piper was running around 800 applications at the time and went through a process afterwards of building them back up. Since the attack, the firm has been running a number of programs to enhance security and business resilience.

Mitigations against ransomware

Malware generally exploits security issues that are publicly known. By keeping your software, and especially your operating system (OS), up to date, you greatly reduce the risk of malware infection[21]. It is equally important to 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.

In addition to the 10 Steps and Small Business Guide, the NCSC has produced some specific guidance on defending your organisation against ransomware attacks:

1. Protect your devices (updates, back-ups).
2. Protect your organisation (defence-in-depth strategy).
3. What to do if your firm has been infected.

Further details can be found here:

- www.ncsc.gov.uk/guidance/mitigating-malware

[20] DLA Piper Head of IT Risk Management

[21] https://www.ncsc.gov.uk/guidance/mitigating-malware

4. Supply chain compromise

Although not unique to the legal sector, supply chain compromises have increased significantly - as much as 200% in 2017[22]. A law firm's supply chain can be compromised in various ways, for example, through the exploitation of third party data stores or software providers.

By far the greatest issue is a third party supplier failing to adequately secure the systems that hold your sensitive data. The increasing use of digital technologies to deliver legal services will likely offer further avenues for exploitation.

Before you can do anything to secure your supply chain you need understand the risks (and benefits) you are taking on by engaging suppliers[23] .

A law firm's position in the supply chain can also make them an attractive target. Cyber criminals can observe the process of a transaction and strike when money is about to be transferred. State actors can also target a law firm as a vector to gain access to corporate clients and their information[24].

[22] https://www.darkreading.com/attacks-breaches/supply-chain-cyberattacks-surged-200--in-2017/d/d-id/1331337

[23] https://www.ncsc.gov.uk/guidance/principles-supply-chain-security

[24] https://www.raconteur.net/technology/defending-the-weakest-link-from-cyberattacks

Case study: cyber actors infiltrate managed service providers[25]

Managed service providers (MSPs) deliver IT, HR, and business services to clients who have outsourced various elements of their infrastructure. They represent a particularly attractive target as they have links to thousands of customers worldwide though private network connections and other relationships.

A known cyber actor was found to have compromised several global MSPs in 2017, although the compromises probably took place at least as early as May 2016. The actor is believed to have intended to obtain commercially sensitive data from the MSPs and their clients.

The compromises are a high-profile example of a supply chain attack, in which a cyber attacker sought to compromise a third party to use it as a stepping stone to the intended target. It is highly likely they will continue targeting MSPs for cyber espionage reasons due to the potential access to companies and governments worldwide.

Even if a client has a strong outward-facing security posture, it may find itself vulnerable if a trusted network link to an MSP is compromised.

Mitigations against supply chain compromise

Law firms must have confidence that their third party suppliers, particularly those that hold their sensitive data, have basic cyber security controls in place. In addition to the 10 Steps and Small Business Guide, the NCSC has produced some specific guidance to help you establish effective control and oversight of your suppliers:

1. Understand the risk.
2. Establish control.
3. Check your arrangements.
4. Continuous improvements.

Further details can be found below:

- www.ncsc.gov.uk/guidance/supply-chain-security
- www.ncsc.gov.uk/guidance/managing-risk-cloud-enabled-products

[25] https://www.ncsc.gov.uk/cyberthreat

Forward look

Around 40 of the 100 biggest UK law firms are already using Artificial Intelligence (AI) systems on active files, four times the number from two years ago .

Legal industry trends[26]

- **Clients**: Continuing need to connect and collaborate through data rooms / deal rooms. Competition for work increasingly based on meeting the needs of clients who challenge the technical capabilities of law firms.
- **Staff**: Growth in the flexibility of legal workforce; use of contract and consulting legal staff and firms. Requirement to have information accessible from anywhere at any time.
- **Delivering legal services**: Expansion of outsourcing services to external suppliers either partially or entirely. Use of automation and robotics to assist with repeatable activities using third party services[27]. Disaggregation of delivering legal services i.e. multi-faceted retainers across multiple firms who specialise but need to work together for clients.

Cyber security trends

- **Targeted intrusion**: malicious activity generally focused on a small set of targets with the intent to steal sensitive data. It is likely that this threat will continue from Nation State actors[28] and serious organised crime groups.

[26] Legal industry trends captured by Industry 100 law firm CISOs

[27] https://www.legalcheek.com/2018/02/rise-of-the-robot-lawyers-law-students-are-embracing-what-the-profession-fears/

[28] https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor

- **Artificial Intelligence (AI)**: the development of computer systems able to perform tasks normally requiring human intelligence, such as decision-making. Around 40 of the 100 biggest UK law firms are already using AI systems on active files, four times the number from two years ago. Around 30 further top law firms are currently piloting systems, and still more are considering a pilot.[29] AI may help with thwarting future attacks, although may also be used maliciously, for example, to fool AI fraud checks or craft high quality phishing emails[30].
- **Blockchain**: a digital ledger in which transactions made in cryptocurrency are recorded chronologically and publicly. As with any new technology, cyber attackers will aim to exploit any potential vulnerabilities. A number of attack vectors, exploiting blockchain ledger architecture using routing and Distributed Denial of Service (DDoS) attacks, have been identified[31].
- **Remote working**: mobile working and remote access extends the transit and storage of information (or operation of systems) outside of the corporate infrastructure, typically over the Internet. Organisations that do not establish sound remote working practices might be vulnerable to the following risks: loss or theft of the device, being overlooked, credential loss and device tampering[32].
- **Risk to smaller firms**: Criminals will always choose the easy target. Even small firms can have significant funds in their client accounts or be acting on sizeable conveyancing transactions, which can make them an attractive target. This makes it imperative that firms, large or small, invest in their staff to make them more cyber aware and resilient.
- **General Data Protection Regulation (GDPR)**: The GDPR requires that personal data must be processed securely using appropriate technical and organisational measures. The regulation does not mandate a specific set of cyber security measures but rather expects you to take 'appropriate' action. What is appropriate for you will depend upon your circumstances as well as the data you are processing and therefore the risks posed, however there is an expectation you have minimal, established security measures in place. The security measures must be designed into your systems at the outset (referred to as Privacy by Design) and maintained effective throughout the life of your system[33] . More information can be found here: https://www.ncsc.gov.uk/GDPR

[29] https://www.thetimes.co.uk/article/top-firms-play-it-smart-with-ai-57qzkkq70

[30] https://www.csoonline.com/article/3250144/machine-learning/6-ways-hackers-will-use-machine-learning-to-launch-attacks.html

[31] https://coincentral.com/blockchain-hacks/

[32] https://www.ncsc.gov.uk/guidance/10-steps-home-and-mobile-working

[33] https://www.ncsc.gov.uk/GDPR

Annex A: Reporting cyber incidents

Action Fraud

Action Fraud is the UK's national fraud and cyber crime reporting centre. If you believe that your organisation has been the victim of fraud, scams or extortion, you should report this through the Action Fraud website: https://www.actionfraud.police.uk/report_fraud . If you are suffering a live cyber attack that is in progress, call 0300 123 2040 now to report. This service is available 24 hours a day, 7 days a week for businesses, organisations and charities.

Information Commissioners Office

The Information Commissioners Office (ICO) is the UK's independent body set up to uphold information rights. Under the new GDPR regulations, from May 2018 organisations that suffer a personal data breach, which is likely to result in a risk to the rights and freedoms of individuals, are legally obliged to report this fact to the ICO: https://ico.org.uk/for-organisations/report-a-breach/ .

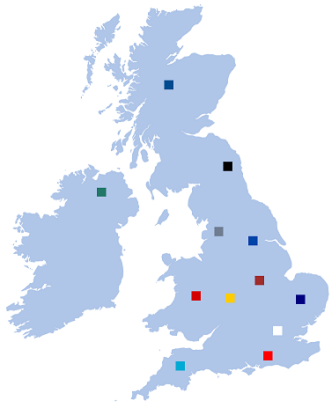
Solicitors Regulation Authority

The Solicitors Regulation Authority (SRA) authorise solicitors and law firms in England and Wales. Solicitors and firms must report breaches of the SRA Code of Conduct to the SRA in line with their regulatory arrangements. This may include reporting a cyber crime that has resulted in a loss of client money or information. Details can be found here: http://www.sra.org.uk/solicitors/enforcement/solicitor-report/other-solicitor-results.page

The NCSC

If you feel you are the victim of a significant cyber security incident you can report this to the NCSC: https://www.ncsc.gov.uk/reporting-cyber-security-incident . Significant includes harm to UK national security, economic prosperity, public confidence, public health and safety or the ability for you to perform the day-to-day running of your business.

Regional Organised Crime Units (ROCUs)



There are nine ROCUs across England and Wales that have a range of specialist policing capabilities. This includes a dedicated cyber security team that works with businesses, organisations, and communities to promote the steps that we think will reduce the chances of becoming a victim of cyber crime.

The ROCUs, and their counterparts in Scotland and Northern Ireland, regularly work with organisations in response to specific threats and can provide support in the event of a cyber incident, irrespective of whether a formal police investigation exists. Their direct link to the NCSC puts them in an ideal position to act as a first point of contact for those that wish to raise their awareness of the cyber threat and improve their defences against attacks. Contact details for your region can be found here: https://www.ncsc.gov.uk/information/regional-organised-crime-units-rocus

Annex B: Small Business Guide actions

Organisations can carry out the following actions in accordance with the guidance contained in the Small Business Guide[34].

Policy actions

These actions should be carried out by staff responsible for determining the overall cyber security policy.

- ☐ Identify and record essential data for regular backups.
- ☐ Create a password policy.
- ☐ Decide what access controls your users need so they can access only the information and systems required for their job role.
- ☐ Decide what staff need access to USB drives
- ☐ Sign up to threat alerts and read cyber local advice e.g. briefing sheets/threat reports from www.actionfraud.police.uk/signup.
- ☐ Create an inventory of approved USB drives and their issued owners, and review whether the ownership is necessary periodically.

Technical actions

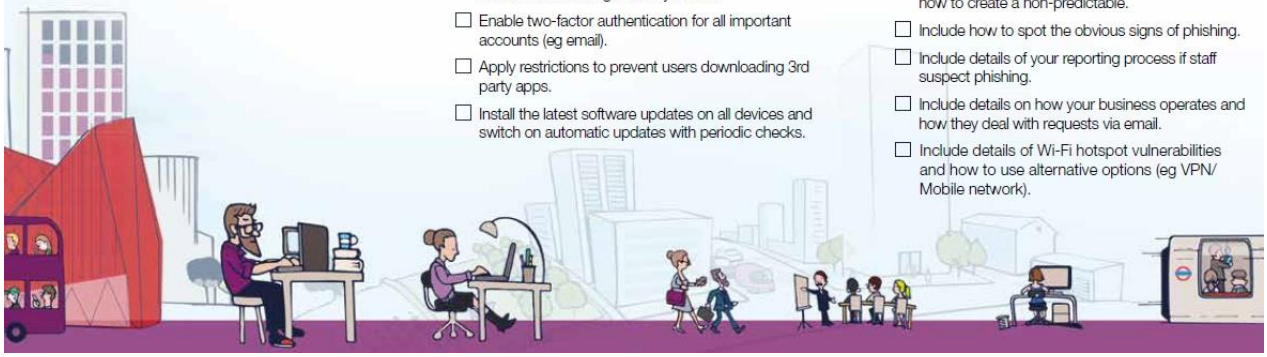
These actions should be carried out by technical staff responsible for the setup and configuration of devices, networks and software.

- ☐ Switch on your Firewall.
- ☐ Install and turn on Anti-virus software.
- ☐ Block access to physical ports for staff who do not need them.
- ☐ Consider making a password manager available to your staff to secure their passwords. Review the star ratings before choosing one from an app store.
- ☐ Ensure data is being backed up to a backup platform e.g. portable hard drive and/or the cloud.
- ☐ Set automated back-up periods relevant to the needs of the business.
- ☐ Switch on password protection for all available devices. Change default passwords on all internet-enabled devices as per password policy.
- ☐ Install and turn on tracking applications for all available devices e.g. Find my iPhone.
- ☐ Enable two-factor authentication for all important accounts (eg email).
- ☐ Apply restrictions to prevent users downloading 3rd party apps.
- ☐ Install the latest software updates on all devices and switch on automatic updates with periodic checks.
- ☐ Ensure all applications on devices are up to date and automatic updates have been set to download as soon as they are released. Schedule regular manual checks on updates.
- ☐ Set up encryption on all office equipment. Use products such as Bitlocker for Windows using a Trusted Platform Module (TPM) with a PIN, or FileVault (on mac OS).

Training and awareness actions

These actions should be carried out by staff responsible for implementing staff training and awareness.

- ☐ Provide secure physical storage (eg a locked cupboard) for your staff to write down and store passwords.
- ☐ Create a Cyber Security training plan that you can use for all staff.
- ☐ Include details of your 'Password' policy explaining how to create a non-predictable.
- ☐ Include how to spot the obvious signs of phishing.
- ☐ Include details of your reporting process if staff suspect phishing.
- ☐ Include details on how your business operates and how they deal with requests via email.
- ☐ Include details of Wi-Fi hotspot vulnerabilities and how to use alternative options (eg VPN/ Mobile network).



[34] https://www.ncsc.gov.uk/guidance/small-business-guide-actions

Annex C: Cyber Security Information Sharing Partnership (CiSP)

The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

UK-based law firms are now able to sign up to a new, private CiSP group tailored to their needs - 'Legal Sector' - which gives access to a wealth of cyber security expertise and advice to help keep you safe online. This group will enable you to communicate and collaborate on cyber security matters with government and industry peers in a secure and trusted environment. We would be delighted for you to join this online community and actively share your knowledge and experience for the benefit of the entire legal industry.

It's free and easy to join. Full details on the membership benefits and joining instructions can be found here: https://www.ncsc.gov.uk/cisp . Part of the sign-up process requires you to register your organisation. The NCSC, the Law Society or the Bold Legal Group can sponsor your organisation, as appropriate.

Annex D: Cyber Essentials

Cyber Essentials[35] is a simple but effective, government-backed scheme that will help you to protect your practice, whatever its size, against a whole range of the most common cyber attacks. It also demonstrates your commitment to cyber security.

From sole practitioners to international corporate firms, Cyber Essentials will help you avoid the consequences of malware, ransomware and phishing attacks. The scheme sets out five controls which are easy to implement, and are designed to guard against these attacks.

1. Use a firewall to secure your Internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware
5. Keep your devices and software up to date

Once implemented you can apply for certification to demonstrate that the controls have been applied correctly. Cyber Essentials certification can help your firm in many ways:

- attract new clients with the promise that you have cyber security measures in place
- reassure clients that you take cyber security seriously
- be listed on NCSC's Directory of organisations awarded Cyber Essentials certification

[35] https://www.cyberessentials.ncsc.gov.uk/

National Cyber Security Centre
a part of GCHQ

The Law Society

National Cyber Security Centre
INDUSTRY 100

The cyber threat to UK legal sector