Cyber Crime:

The risks facing the UK Legal Profession

Author

Nicola Anthony | Risk & Compliance
T +44 20 7031 2791
E nicola.anthony@miller-insurance.com

Key contacts

Ed Pickard | Head of UK Professions
T +44 20 7031 2962
E ed.pickard@miller-insurance.com

Tim Jackson | UK Professions
T +44 20 7031 2816
E tim.jackson@miller-insurance.com

Zarina Lawley | Head of Solicitors PI
T +44 20 7031 2491
E zarina.lawley@miller-insurance.com

The Solicitors Regulation Authority (SRA) recently published its **thematic review on cyber security**, detailing findings in five key areas, namely, cyberattacks, people, technology, support and reporting. A review of a sample of 40 law firms was undertaken to understand the different types of cyberattacks, what measures were (or were not) in place at the time of the attack as well as the resulting impact.

This article is designed to highlight the key areas you should be aware of as well as providing useful mitigation tips and strategies.

With COVID-19 and the existing restrictions in place, there are an extensive number of company employees working remotely; therefore, there is a greater emphasis required on cybersecurity for all members of staff to be vigilante and provided with the necessary training and support to help prevent a cyberattack. "For firms, having knowledgeable and empowered staff is the first line of defence against cybercrime." 60% of the sampled firms believed that staff were the greatest cyber risk. Along with effective training, having effective policies, procedures and controls in place that respond and mitigate an attack, can also assist in the fight against cybercrime.

Cyberattacks:

Types of attacks:

- Email modification
- Spyware
- Ransomware
- Viruses
- Denial service attacks
- Gaining remote access to a firm's systems

Volume and impact of attacks:

- 30 of the 40 firms had been the target of a cyberattack.
- 23 of the 30 cases in which firms were directly targeted saw a total of more than £4m of client money stolen.
- Of the £4m lost, £3,665,799 was claimed against insurance policies, a further £393,890 had to be paid out by 18 firms from the firms' own money. These figures do not take into account the wider costs ramifications; higher insurance premiums, lost time, damage to client relationships.
- £150,000 lost in billable hours following a ransomware attack, initiated accidentally by a fee earner, which crippled their systems.
- Two large law firms were targeted more than 100 times each year.
- 31 firms had been successfully targeted.

Most incidents occurred due to employee errors and misunderstanding rather than systems being hacked.

Mitigation is key to reduce the risk of a cyberattack. 23 of the 40 firms reviewed later introduced more than one measure; either creating or changing existing controls/process/policy. The mitigation introduced was deemed effective and appropriate in preventing further incidents in 92% of the matters investigated.

People:

- 24 of the 40 firms (60%) sampled believed that staff knowledge and behaviour was the greatest cyber risk.
- 33% considered e-mail interception as one of the greatest risks.
- 8 of the 40 firms visited had never provided specific cyber security training to their staff.

Types of policies firms have developed:

- Cyber security
- Website and social media policies
- Card payments
- Email usage
- Passwords

Knowledge and empowering staff is key to preventing a catastrophic cyber incident, therefore providing appropriate training to your staff plays a pivotal role. Within the review, many firms reported that various incidents occurred with administrative support, finance and IT staff. Therefore, training should be provided to all members of staff, with complexity and how training is rolled out relevant to the role of the individual. We recommend keeping a record of all training and updates to policies, procedures and controls; keeping those under review will ensure that all staff are kept abreast to changes and new threats.

The SRA also reported that firms implemented policies and procedures relevant to client-based risks:

- Telling clients that bank details wouldn't change
- Not providing bank details by email
- Asking clients not to send money until it was requested
- Reminding clients about their use of social media and the information they share.

Providing clients with a simple fact sheet including such information provides them with knowledge on cybercrime, helping to prevent a potential attack.

Disaster recovery plan

Policies/procedures/controls are not bullet proof, so having a Disaster Recovery Plan is a good idea to respond quickly to an attack. It is recommended that time is taken to compile relevant information such as contact details and telephone numbers and emergency processes, and consider where the document will be saved (i.e. not on the system that may become compromised). The thematic review reported that:

- 14 of the 40 firms had taken no steps to test or audit their processes and/or procedures.
- 27 firms had produced disaster recovery plans, with 15 firms storing the document on the same system that could be unavailable following an attack.
- 19 firms had undergone penetration testing by an external party. They test the security, vulnerability and robustness of a firm's software.
- 15 firms had taken internal steps to stress test processes and procedures; mock cyberattacks and testing staff with phishing emails.

Technology:

- 93% of the firms visited had firewalls in place.
- 25 of the 40 firms had two-factor authentication requirement for staff/clients when engaging in day-to-day activities. The two-factor authentication is recommended by Cyber Essentials for extra security. "For important accounts such as banking and IT administration, you should use two factor authentication, also known as 2FA. A common and effective example of this involves a code sent to your smartphone which you must enter in addition to your password."

All firms undertook some form of data backup and confirmed that their laptops and devices were password protected. However, there were vulnerabilities identified;

- More than half of the firms allowed external data sticks to be freely used and plugged into their machines.
- 2 firms used an old Windows operating system – where security updates had ceased in 2014.
- 16 firms were using a system where Windows support was due to end imminently.

Cybercriminals will look to exploit vulnerabilities in your systems, and therefore you should avoid using data sticks, and ensure you use the latest version of operating systems and browsers.

Cyber Essentials is a government backed scheme that helps businesses guard against the most common cyber threats. Cyber Essentials can assist in protecting your firm and recommends using six technical controls:

- Use a firewall
- Choose the most secure settings for your devices and software
- Control who has access to your data and services
- Protect yourself from viruses and other malware
- Keep your devices and software up to date
- Conclusion and checklists.

Support:

- 30 of the 40 firms sampled relied on help from commercial IT specialists; whilst this is positive, firms should ensure that they are not totally reliant on this.
- 12 firms had cybercrime insurance.
- 5 firms had Cyber Essentials Plus accreditation.

The review found that those who did have the Cyber Essentials accreditation were more likely to have good policies and procedures in place, and taken effective steps to protect themselves against cybercrime.

Reporting:

- ***Solicitors Regulation Authority (SRA)*** - Any successful cyberattacks should be reported to the SRA.
- ***Information Commissioner's Office (ICO)*** – If a personal data breach occurs, firms must report this to the ICO within 72 hours where they consider there being a risk to an individual's rights and freedom.
- ***Law enforcement*** – A report should be made to Action Fraud where you have experienced cybercrime.

Of the firms sampled in the review; on three occasions firms did not contact law enforcement despite serious incidents and losses of client money;

- A client transferred £70,000 to a fraudster.
- Another client made a further £70,000 transfer to a fraudster in an unrelated incident.
- A solicitor transferred £340,000 to a fraudster.

It is worth noting that it is not detailed within the review the types of attacks that were the cause of these losses. However, email modification frauds are the likely suspect, with bank details changed once the fraudster had intercepted the email chain, and the monies sent to the wrong accounts, unbeknown to the client/solicitor.

Reporting of cyberattacks where the client was affected, but the firm had not been, is not a regulatory requirement, but, it is encouraged by the SRA to assist with tackling cybercrime, and raising awareness.

Cyber Insurance:

The review touches on cyber insurance, with 12 of the 40 firms sampled having cyber insurance in place and detailing a range of other benefits, namely:

- Emergency contact information
- Help with training
- Help with analysing firm risk
- Access to specialist advice and teams.

Cyber insurance is designed to protect you against cyber and data privacy losses.

What is covered?

- Claims from third parties
- Costs of defending any regulatory proceedings
- Losses you may suffer as a result of a cyber event
- The costs and expenses of the incident response.

There are four broad categories of loss arising from a cyber-event:

- Cyber Liability
- Privacy Breach
- Non-physical damage business interruption
- Cyber Extortion

Why the need for cyber insurance?

Cyber insurance provides cover for emergency response to a cyber-event and first party loss. The speed of a response to a cyber-event and your reputation is everything in how effective and efficient such events are managed. With cybercrime on the increase; cyber insurance is more important than ever, for the reasons detailed above; and in particular the emergency response services (Legal/regulatory, IT forensics, Cyber extortion, PR consultancy, Credit monitoring/notification management), which most cyber policies provide and the first party cover (firms own losses), which is not provided by your professional indemnity insurance.

To conclude, firms should ensure they remain vigilante and that all staff have the appropriate training to be able to identify and potentially prevent a catastrophic cyber incident occurring to your firm.

Useful links:

NCSC: https://www.ncsc.gov.uk/collection/passwords

Cyber Essentials: https://www.ncsc.gov.uk/cyberessentials/overview

Law Society Cyber Group: https://www.lawsociety.org.uk/topics/cybersecurity

Action Fraud: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

About Miller

Since Miller was founded in 1902, we have gone from strength to strength because of our unwavering focus on delivering an exceptional standard of service to our clients.

We are known for doing the right thing, delivering on our promises and working as one team.

Today, we are a leading specialist (re)insurance broking partnership, headquartered in London with more than 650 people across our UK and international operations.

We are Chartered Insurance Brokers, publicly committed to a customer-first approach and values that align with a professional Code of Ethics. We'll provide solutions relevant to your needs, maintaining our knowledge through qualifications and ongoing professional development.

This material is for general information purposes only. Please speak to us directly to discuss your specific insurance needs. Miller Insurance Services LLP is a limited liability partnership registered in England and Wales; Registered Number: OC301468; Registered Office: 70 Mark Lane, London, EC3R 7NQ. Authorised and regulated by the Financial Conduct Authority. Miller Europe SPRL est une société privée à responsabilité limitée de droit belge; Val d'Or, Gulledelle 96, 1200 Bruxelles, Belgique 0708.954.984 (RPM Bruxelles); Inscription FSMA 0708.954.984. IBAN: BE46949007962036. Succursale de Paris, 40 rue La Pérouse, 75116 Paris, RCS Paris 849 440 458. London branch is registered in England and Wales; Registered Number: BR021148. Registered Office: 70 Mark Lane, London, EC3R 7NQ. Authorised by the Belgian Financial Services and Markets Authority. P483.06 1220 | © Miller 2020