Law Firms and Cyber Security: the 4 most common cyber threats

Submitted by: PR Artistry Limited
Thursday, 24 September 2020

Data breaches are becoming more prevalent and the legal sector is a favoured target and is falling victim to cyber-attacks at an alarming rate. Guy Lloyd at CySure explains the 4 most common cyber threats and why the legal sector should step up its focus on cyber security.

As data controllers, law firms handle significant volumes of confidential and sensitive information, as well as vast amounts of client funds as part of their daily work. The legal sector is increasingly reliant on technology to conduct its day to day activities. However, many law firms have been slow to put basic cyber security controls in place and as a result are falling victim to a range of malicious cyber activity. Post GDPR, legal firms cannot afford to be complacent about cyber threats. Breaches can affect a company's stability and severely damage its reputation.

Cyber-attacks continue to occur despite the National Cyber Security Centre (NCSC) issuing its first legal threat report (i) in 2018 warning of the threats in the legal sector. At the time, it reported that £11 million of client money was stolen due to cyber-crime between 2016 and 2017. Today the statistics are even more alarming.

According to a 2019 report on fraud and cyber-crime vulnerabilities in the legal sector (ii), law firms in the UK remain susceptible to cyber attacks.
• 91% of firms are exposed to having their website addresses spoofed and used to send spam, phishing or otherwise fraudulent emails
• 80.5% of firms were running at least one service, such as an email server or webserver, with a well-known vulnerability that could be exploited by hackers
• 21% of firms had at least one service that was using software which was out of date and no longer supported by the developer, putting them at higher risk of attack and service failure.

Therefore, what are the most significant cyber threats that law firms should be aware of?

Phishing – both indiscriminate trawling and line phishing

Phishing is the most common cyber-attack affecting law firms and is particularly prevalent in areas such as conveyancing. 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. A poll of law firms showed that approximately 80% have reported phishing attempts (iii). Phishing is a relatively low cost/low tech attack but carries a high reward, making it a popular and lucrative method for cyber criminals.

Data Breaches – theft of data and hacking of client accounts

The loss of client information can have a devastating reputational impact on a sector that has confidentiality at the heart of its business. Data breaches can occur through theft of data and hacking of office or client accounts. However, law firms need to wise up to the risk of the insider threat – both accidental and malicious. The latter can come from an employee seeking financial gain or with a grievance against the firm. According to The Industry Security Forum, over half of all data breaches are

caused by insiders (iv).

1. Ransomware – access denial

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 (v). Paying the ransom does not guarantee that you will get access to your data/device because attackers may assume that you would be open to paying ransoms in the future. Whilst ransomware is a problem for all businesses, the very nature of the work that law firms do makes them an especially vulnerable target. Many law firms are reluctant to believe they will ever be attacked in this way. However, this belief coupled with the low level of IT resources typically able to address security issues exposes law firms to widespread business disruption.

2. Supply chain disruption

Supply chain compromises are not unique to the legal sector but as a threat, they are increasing. A law firm's supply chain can be compromised in several ways but the most common is a third party supplier failing to adequately secure the systems that hold a firms sensitive data. The increasing use of digital technologies to deliver legal services offers further avenues for exploitation. Before law firms can do anything to secure their supply chain, they need to understand the risks and have confidence in their third-party suppliers. It’s important for law firms to establish effective control and oversight of their suppliers and ensure they have basic cyber security controls in place.

Cyber security can no longer be an afterthought

It is time for the legal sector to take cyber security seriously. Failing to do so will only lead to devastating repercussions in the not-so-distant future. Make your firm a tougher target by becoming certified with Cyber Essentials. Cyber Essentials is a government and industry backed certification scheme. It sets out basic technical controls for organisations to use which are then annually assessed. It also lays the foundation to developing policies and procedures to mitigate against threats that can impact business operations. Being fully Cyber Essentials compliant is said to mitigate 80% of the risks faced by businesses such as phishing, malware infections, social engineering attacks and hacking. Using an online information security management system (ISMS) that incorporates GDPR and Cyber Essentials Plus is a simple and cost-effective way to carry out a gap analysis and highlight the areas that your business needs to focus on.

Educate employees

One of the most effective defences against cyber-crime is to help employees understand how attacks happen. It makes sense to train them to recognise spam and other phishing techniques, so they don’t get fooled into enabling a cyber-attack. In addition, ensure procedures are in place as to what should be done in the event of the worst happening.

Information management security systems such as CySure’s provides businesses with a staged approach to compliance and certification. Guided by CySure’s virtual online security officer (VOSO) firms have a low-cost way to proactively protect themselves against a whole range of the most common cyber-attacks. For more information visit CySure (https://cysure.ltd/voso/)

(i) NCSC (https://www.ncsc.gov.uk/news/cyber-security-advice-issued-law-firms-first-legal-threat-report)

(ii) Kynd.io
(https://www.kynd.io/wp-content/uploads/2019/11/Fraud-and-cybercrime-vulnerabilities-in-the-legal-sector-FINAL.pdf)
(iii) Law Society research: online cybersecurity poll, June 2018 and i100 partners
(iv) Security Forum (https://www.securityforum.org/research/managing-the-insf-briefing-paper/)
(v) Lawyers defence Group (https://www.lawyersdefencegroup.org.uk/ransomware/)

About CySure

CySure is a cyber security company founded by experts with extensive experience in operational and risk management. The company has offices in London (UK) and California (USA) and CySure's flagship solution – Virtual Online Security Officer (VOSO) is an information security management system (ISMS) that incorporates GDPR, US NIST and UK CE cyber security standards to guide organisations through complex, emerging safety procedures and protocols, improve their online security and reduce the risk of cyber threats.

For more information please visit www.cysure.ltd
Press contact: Mary Phillips/Andreina West
PR Artistry Limited
T: +44 (0)1491 845553
E: mary@pra-ltd.co.uk