Are law firms being proactive enough when it comes to cyber security?

Submitted by: PR Artistry Limited
Tuesday, 16 February 2021

5 steps to getting started

Lockdown working has exposed the gaps in cyber security practices in many law firms. With hackers looking for a pay day, it's never too late to become cyber proactive. Guy Lloyd at CySure explains why cyber security doesn't need to be complex, costly or confusing.

Law firms are privy to a huge amount of sensitive client data and handle vast amounts of money in daily transactions, mostly conducted online. Whilst many firms have ticked what they think are the right boxes in terms of cyber security, the number of cyber threats targeting law firms tells a different tale. A recent cyber security review published by the Solicitors Regulation Authority (SRA) reported that three quarters (i]) of the firms visited and interviewed said they had been the target of a cyberattack. The remaining quarter of firms reported that cybercriminals had directly targeted their clients during a legal transaction.

In the digital age, a law firm without cyber security measures is an easy target for hackers looking for victims. To highlight the significant risk to law firms, the National Cyber Security Centre (NCSC) published its first report into the cyber threat to the UK legal sector (ii). The challenge for many firms is that security is not a core area of business and it can be a struggle to justify the cost of hiring security expertise. So, what can law firms do to protect their reputations as well as their client's confidential data and money?

1. Understand your risk – to reduce exposure to cybercrime, it's important to understand the risks your firm is facing and develop controls, process and policies to mitigate them. It needs to be clear to all employees who is the person responsible for the cybercrime defence policy at the firm and what processes and controls are in place. When the worst-case scenario happens, it's vital that employees know what to do and who to contact. The eye of the storm is not the moment to be trying to work out who is doing what.

2. Take ownership – the SRA report highlighted that 75% of firms questioned predominantly relied on help from commercial IT specialists. Whilst security service providers can be a source of valuable expertise, firms should beware of becoming completely reliant on their guidance. This point was underlined in the SRA report by legal firms that had received poor advice from third-party providers, which ultimately left them exposed to fraudsters. Managing and defining risk has to be owned by the company as a whole and understood by the leadership team - it can't be outsourced. No one else will know your business with the same depth of knowledge or care about it as much as you.

3. Build a security aware culture – the ability to prevent and mitigate cybercrime depends on everyone within a firm having a good level of awareness about cyber security. Having knowledgeable and empowered staff is the first and best line of defence against cybercrime. Creating a culture that mirrors good cyber hygiene relies upon having effective policies and controls in place. Cybercriminal try to trick their victims into making mistakes but if employees are trained on common scams to look out for, such as phishing emails and rogue websites, your firm will already have a head start.

4. Understand your responsibility to securing data – if your practice collects, stores or uses EU citizens' personal data it is subject to GDPR. To be GDPR compliant there must be basic data security controls in place such as those specified by the National Cyber Security Centre's (NCSC) Cyber Essentials policy. Law firms cannot afford to be naïve or negligent about their data responsibility due to the confidential and highly personal data they store. The Information Commissioner's Office (ICO) has produced a checklist to help companies understand their responsibilities (iii). If there are doubts about your firm's ability to adhere to GDPR's 'security principle', now is the time to act.

5. Be prepared – the undeniable fact is the legal sector is an attractive prospect to hackers and statistically legal firms are highly likely to be targeted. Preparation is key and this is where Cyber Essentials (CE) certification is invaluable. CE is the National Cyber Security Centre's assurance product aimed to help protect UK organisations from the most common cyber threats. The scheme 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. Market forces have a way of punishing businesses who fail to prepare. Act now and demonstrate commitment to cyber security by achieving CE certification.

Can you afford to be a sitting duck?
Cyber criminals have no morals or ethics, attacks are not personal, although it can feel that way when it's your firm that is facing the aftermath of an attack. Cybercrime is mostly financially motivated as hackers want a quick pay day and seek out easy targets. Don't be a sitting duck. No firm is too small to be a target or to mount a defence against cybercrime. CE certification will put you on the right path to implementing cyber security controls. Being CE compliant is said to mitigate 80% of the risks faced by businesses such as phishing, malware infections, social engineering attacks and hacking. However, should the worse happen, CE will aid in the ability to respond to a cyberattack and resume business operations.

Getting started can seem daunting but achieving certification doesn't have to be. Using an online cyber security policy management system that incorporates GDPR and Cyber Essentials is a simple and cost-effective way to achieve certification. Look out for a solution that can carry out a gap analysis and underline the areas that your business should focus on. Taking these steps can go a long way to protect against common attacks. It's also a far more effective strategy than closing your eyes, crossing your fingers and hoping that your firm won't be the next victim.

Guy Lloyd – Director at CySure

(i) SRA: Cyber Security Thematic Review 2020
(ii) NCSC - The Cyber Threat to UK Legal Sector Report
(iii)ICO
(https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/)

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 CySure's flagship solution – Cyber Security Policy Manager (CSPM) is a policy management system 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 CySure (http://www.cysure.ltd)

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