Cyber threat to the legal sector: 6 proactive steps to take now

Joe Collinwood, CEO at CySure highlights the risks of weak cyber security and advises on how to mitigate exposure.

LONDON, UK, September 25, 2019 /EINPresswire.com/ -- The primary threat to the legal sector stems from cyber criminals with a financial motive. However, increasingly the hacktivist community is targeting law firms to achieve political, economic or ideological ends.

Criminals are attracted to the legal sector because of the vast amounts of valuable data legal firms hold. New client intake procedures require checking personal identifying information such as passports, bank statements, tax statements and social security numbers. For corporate clients, law firms hold commercially sensitive information on mergers and acquisitions, contracts and intellectual property. All this data is profitable currency in the wrong hands.

> “The financial and reputational impact of cyber attacks on law firms is significant - from the costs that arise from the attack itself and then repairing reputational damage to regain public trust ”
>
> *Joe Collinwood, CEO, CySure*

The responsibility for cyber security can often fall through the gaps as lawyers are not necessarily trained IT security experts. Not having an owner for the firm’s cyber security strategy can lead to a lack of effective and continually reviewed processes, leaving firms wide open to the risk of attack.

According to the 2018 PricewaterhouseCoopers Law Firm survey , 60% of firms reported suffering a security incident during the year. The financial and reputational impact of cyber attacks on law firms is significant. The costs that arise from the attack itself and then repairing reputational damage to regain public trust can be considerable.

Friday afternoon fraud
The Solicitors Regulation Authority (SRA) Risk Outlook 2017/2018 in the UK revealed that from the first quarter of 2016 to the end of the first quarter of 2017, solicitors reported over £12m of client money stolen by cyber criminals. A total of 80% of all cyber crime reports to the SRA in the second quarter of 2018 were related to email modification fraud, where criminals intercept and falsify emails between a client and firm leading to bank details being changed and money being lost. When used to steal conveyancing money it is also known as 'Friday afternoon fraud', as many of these transactions take place on Friday afternoons.

It’s not just conveyancing practices that need to be on their guard.
Legal firms can no longer afford for cyber security to be an afterthought, here are 6 proactive steps organizations can take to improve their cyber defences before it is too late:

1. Assess your current cyber risk levels
Unless there is awareness of the potential risks then it is almost impossible to create a strategy

for minimising them. Certification provides a practical framework for an organization to assess its current cyber hygiene levels. In the UK, Cyber Essentials is a government and industry backed scheme to help all organizations protect themselves against common cyber-attacks. In collaboration with Information Assurance for Small and Medium Enterprises (IAMSE), they set out basic technical controls for organizations to use which is annually assessed. In the US the National Institute Standards and Technology (NIST) framework guides organizations through complex, emerging safety procedures and protocols.

Being fully Cyber Essentials compliant is said to mitigate 80% of the risks faced by businesses such as malware infections, social engineering attacks and hacking. By utilising an online information security management system (ISMS) that incorporates NIST and Cyber Essentials Plus, legal practices can undertake certification, guided by a virtual online security officer (VOSO), as part of its wider cyber security measures.

2. Practice good cyber hygiene
Good cyber hygiene is about getting the basics right and proactively offsetting the identifiable risks. Invest in effective firewalls, anti-virus and anti-malware solutions and ensure updates and patches are applied regularly. The National Cyber Security Centre advises updating software as soon as a new patch or update is available. Additionally, user passwords should be changed regularly and unused or end-of-life equipment disposed of securely.

3. Secure and back up data
Losing the ability to restore business critical data after an incident can be catastrophic to a business. Data loss can damage reputations and paralyse operations and since the General Data Protection Regulation (GDPR) came into force on 25 May 2018, organizations can face hefty fines should they suffer a data breach. Organizations should ensure business critical data on all company assets is securely backed up and can be quickly restored.

4. Develop effective policies, processes and incident response plans
Organizations should have simple and clear policies in place, communicated to all personnel so they are familiar with current processes. It is also essential to have an up-to-date incident response plan that is practised regularly so that employees know what to do when they suspect there is an attempted breach or if an actual incident occurs. With GDPR now in force, it is important for firms to quickly identify and understand the nature and level of breaches and to have a plan to deal with reportable events.

5. Consider the human element
Regular awareness training of employees is vital to combat common scams, such as phishing which is the most common cyber attack impacting law firms. A recent poll conducted by the UK Law Society showed that approximately 80% of firms have reported phishing attempts in the last year . By engaging in regular cyber security training, firms can raise awareness with employees of the potential scams or tactics being used to trick them.

6. Invest in cyber insurance
Consider investing in cyber insurance to cover the unique exposure of data privacy and security. Standard policies are often inadequate to cover the likely cost of a security breach, whereas specialist cyber insurance policies provide comprehensive cover for cyber attacks and hacktivism.

The cyber threat to the legal sector is not going away. Regardless of the national regulatory standard your firm chooses to follow, either CE or NIST, it is time to be proactive in terms of protecting your own data and that of your clients.

Joe Collinwood is CEO of CySure

(i) https://www.pwc.co.uk/industries/business-services/law-firms/survey.html

(ii) https://www.sra.org.uk/risk/outlook/risk-outlook-2017-2018.page

(iii) Law Society research: online cybersecurity poll, June 2018 and i100 partners

Mary Phillips
PR Artistry
+44 1491 845553
email us here