Law firms and cyber crime

The growing threat towards the UK legal sector

CORVID

60%

of law firms reported an information security incident in the last year; an increase of 20% YOY.[1]

£11m

was stolen due to cyber crime in 2016-17; the Solicitors Regulation Authority (SRA) reports.[1]

Cyber crime is a growing concern for all businesses across every industry.
Even more so for those who operate in vulnerable sectors, such as law firms. The latest threat report from the NCSC highlighted the rising cyber security concerns and the UK legal sector's attractiveness to cyber criminals.

Law firms, as with all modern day working practices, are reliant on technology. We live in a digital economy where flexible working, 24/7 access to information and online transactions are the norm. The sheer amount of connectivity expected makes everyone vulnerable. The Department for Digital, Culture, Media and Sport undertook a cyber security breaches survey earlier this year and from their research, 98% of all types of UK businesses rely on some form of digital communication or services,[2] which exemplifies the scale of why cyber security should be a high priority.

The numbers

Recent figures are alarming. Particularly so for legal firms who admit they need greater awareness of cyber security. Christina Blacklaws, President, The Law Society mentioned in the threat report;

"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."[3]

Although there is a plethora of resources available, the sector struggles to understand cyber threat. 60% of law firms in 2017 reported an incident, but that's only those who identified a problem. There has been a 42% increase in reported incidents since 2014.[4] This could mean either businesses are more aware so are reporting cases, or, cyber crime is on the rise. Most likely a combination of both.

Profiling law firms

The legal sector is particularly vulnerable due to the volumes of data, sensitive information, financial responsibility and authority they hold. If the law firm specialises in Corporate law or Property law, then they are at a greater risk; as the financial gain is unprecedented.

As highlighted in the threat report, the main reason law firms are targeted is for financial gain; but there is a growth in cyber adversaries achieving political, economic or ideological ends.

Law firms are also often perceived to be an easy target. Smaller firms in particular, as they don't have the same resources as larger practices, but still hold significant funds. Also, they most likely have a small team managing their entire business infrastructure, with limited IT security resources available.

It is often misconstrued that cyber security is undertaken by the IT department; but the truth is, every department is accountable. Cyber security is part of the bigger Information Risk Management and it requires emphasis from business leaders.

Impact of falling foul

The implications of a cyber attack to any business is detrimental, even more so when your business mentality and core service is built on trust and discretion. Not only do law firms and their clients have the financial impact, risk of loss in earnings and business services; but the reputational damage for the practice can be irreversible.

Therefore, to ensure the law firm is protected and to keep their own and client data/intellectual property (IP) secure, they need to be aware of the following cyber security threats. These three were identified in the NCSC report as being the most significant to the legal sector.

Cyber threats to be aware of

1 Phishing

Email is the main route for this type of social engineering cyber attack. Phishing scams can include impersonation, intercepted emails and, or, malicious attachments. The aim of threat actors, those responsible for the attack, is to provoke users to make a mistake, such as: disclose sensitive information, provide users credentials or download malware.

"The most common security incidents continue to be phishing attacks. 12% of firms claim to be recipients of such attacks on a daily basis with a further 30% identifying attacks on either a weekly or monthly basis." PWC Law Firms' Survey Report 2017.

2 Ransomware

This type of threat locks users out of systems and accessing data, with adversaries demanding payment for decryption; although there is no guarantee that paying the ransom will resume normality. Financial gain is the predominant motive behind these cyber attacks; however, with the rise in organised crime, threat actors are also looking to cause disruption to earn respect within the hacktivist network.

DLA Piper, one of the world's biggest law firms, suffered a Petya cyber attack on the 27th June 2017. It is a prime example exemplifying the consequences of falling foul to a ransomware attack.

"For two days after the attack all telephones and emails at DLA Piper, which has about 3,600 lawyers in 40 countries, including in Kiev, the Ukrainian Capital, were knocked out… nine days on from the attack, it [had] not managed to regain complete access to emails sent or received before the ransomware struck… On July 2, it issued a statement to say it [had] 'brought our email safely back online, and continue to bring other systems online in a secure manner'."[5]

DLA Piper is a practice that provides cyber security advice and manages thousands of client accounts. As a result of the compromise, firstly to repair the reputational damage would be enormous, but to also suffer such a long period of downtime, the financial losses would be extortionate. The DLA Piper financial impact was estimated to be in the millions.[6]

3 Supply chain compromise

Cyber criminals are attracted to easy targets. They will always go for the weakest part in the chain, often a third party supplier; this is a supply chain compromise. Cyber adversaries look to harvest information, intersect business transactions and exploit vulnerabilities.

For example, law firms can be targeted by these types of cyber attacks in two ways;

1. Their supply chain can be targeted; such as a data centre to extract client information
2. They are the link in the supply chain; e.g. cyber criminals could impersonate their domain to affiliate financial transactions to themselves

Footnotes

[1] https://www.ncsc.gov.uk/blog-post/new-ncsc-report-highlights-threats-uk-legal-sector | [2] 'Cyber Security Breaches Survey 2018: Statistical Release; Department for Digital, Culture, Media & Sport, Ipsos MORI and University of Plymouth, April 2018 | [3] 'The cyber threat to UK legal sector' threat report; NCSC, The Law Society and NCSC Industry 100, July 2018 | [4] https://www.pwc.co.uk/industries/law-firms/law-firms-survey-report-2017.pdf | [5] https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895 | [6] https://www.legalweek.com/sites/legalweek/2017/07/07/dla-piper-hack-could-cost-millions-brokers-say/?slreturn=20180807072258

Next steps

Take action and be prepared. As touched upon earlier, there is an abundance of resources available to help practices adopt a cyber security mind-set. The recent legal sector threat report from the NCSC being one of them, its purpose to raise awareness and highlight safeguards that can be put in place.

Law firms can also choose to work with a Managed Security Service Provider (MSSP). The benefit to working with an expert is they will help reduce your attack surface, limiting vulnerabilities and providing complete peace of mind for your IT security. They implement the right cyber protection to achieve and maintain low risk. Law firms who operate with extremely sensitive material and are therefore considered highly vulnerable should choose to partner with a MSSP. A recent post on the subject of understanding the value of a MSSP can provide some further useful reading.

Also speak to peers. The Law Society offers a good support network and is a worthy first port of call.

Speak to an expert

This is where Corvid can help. The team, live and breathe cyber. They understand that one size doesn't fit all when it comes to cyber security. They take the time to understand business objectives, concerns and risks. Then provide the right cyber security solution to solve the problem; be it email protection, malware hunting, vulnerability scanning or internet security. Coupled with timely intelligence, Corvid will ensure comprehensive continuous protection from cyber attacks. Get in touch to start the process.

GET IN TOUCH

CORVID

About Corvid

Cyber attacks are growing in severity and sophistication. Attackers are well resourced, clever and highly motivated, often understanding aspects of security technology better than IT managers. The scale of the threat to organisations is huge.

That's where Corvid can help.

We're a growing team of cyber security experts, developers and analysts based in Cheltenham, UK, who are passionate about delivering innovative, robust and extensive defence systems to help protect businesses against cyber threats.

From enhanced email protection to malware hunting or network defence, our range of cyber security solutions are designed to meet the threats facing businesses today.

FIND OUT MORE