The cyber threat to the UK legal sector

The National Cyber Security Centre’s July 2018 report focuses on the cyber risks law firms face. We summarise the key findings below.

Facts and figures

According to a 2017 PWC survey, 60% of law firms reported an information security incident in the last year, up from 42% in 2014. The SRA reports that (i) over £11 million of client money was stolen due to cybercrime in 2016 and 2017 (ii) approximately 80% of law firms have reported phishing attempts in the past year and (iii) the amount stolen from law firms through phishing in the first quarter of 2017 was 300% higher than the previous year.

The report by the National Cyber Security Centre

As data controllers, law firms handle substantial volumes of confidential and sensitive information putting them at risk of data breaches and related GDPR consequences. Many law firms also hold significant client monies putting them at risk from first and third party cyber fraudsters. Law firms need to ensure their employees are cyber-aware as to their data obligations and the common forms of cyber fraud. A link to the full report can be found here.

Common threats to law firms

The most significant cyber threats that law firms face are:

1. Phishing
2. Data breaches
3. Ransomware
4. Supply chain compromise
Phishing

Phishing is a type of social engineering where attackers influence users to reveal sensitive information such as usernames, passwords and card payment numbers online, usually by email. By way of example, PayPal or Apple users may receive an email which instructs them to click on a link in order to rectify a discrepancy with their account. In reality, the link leads to a fake login page that collects the user’s login details.

The NCSC has produced specific guidance on how to defend an organisation against phishing, including:

+ Implementing processes to verify (via independent means) invoices and account details for money transfers;
+ Using 'cooling off' periods for changing account details for high value transactions;
+ Encouraging a culture where suspicious transactions are queried or improperly validated payments are refused; and
+ Educating the firm about the firm’s invoice and money transfer process.

Data breach

Information held by law firms is often politically or commercially sensitive. Where most communication is sent by email, including privileged documents, it makes law firms particularly exposed to the risk of data breaches. In 2016, Panama based law firm Mossack Fonseca suffered a major data breach commonly known as the Panama Papers hack. The impact of the breach was significant and undoubtedly a big wake up call to law firms.

Ransomware

Ransomware is malware that prevents users from accessing their system and data until ransom money is paid, usually by bitcoin. Attackers have become increasingly sophisticated with the development of ransom cryptware, which encrypts files with a private key that only attackers possess.

Law firms are an attractive target for ransomware attacks given their size and financial capability to pay ransom monies. For example, in 2017, law firm DLA Piper suffered a global ransomware attack which caused business disruption for a number of weeks.
The NCSC has produced detailed guidance on how an organisation can guard itself from ransomware attacks. Further details can be found here.

Supply chain compromise

A law firm’s supply chain can be compromised in various ways. For example, law firms may outsource their IT, HR, Finance or other business services to Managed Services Providers (MSPs). Such MSPs are an attractive target to cyber-attacks because they have links to thousands of customers worldwide through private networks and various other relationships. The big issue for law firms is ensuring that the MSPs have systems that are adequately secure to hold sensitive data. Even where a law firm has strong internal security, it may find itself susceptible to a cyber-attack where a trusted network linked MSP is compromised.

Concluding remarks

Cyber security is a crucial business issue for all law firms and needs to be taken seriously at senior management level. In the new GDPR world as well as immediate financial, SRA regulatory and reputational issues, law firms also face potential significant uninsurable fines arising from cyber problems. Law firms should review the full NSCS report and ensure that they have robust plans in place to protect their client data and monies.

July 2018

For further information please contact:

Stephen Reilly
Partner
T: +44 (0)20 7469 0419
E: s.reilly@beale-law.com

Sophie-Rose Bowen
Trainee Solicitor
T: +44 (0)20 7469 0413
E: s.bowen@beale-law.com