UK law firms admit gaps in training and preparation against cyberattacks, Menlo Security research reveals

Submitted by: Origin Comms Ltd
Monday, 23 May 2022

New research (https://info.menlosecurity.com/rs/281-OWV-899/images/IRN-Menlo-Cybersecurity-Legal-Research%20Report-May-22.pdf) among 150 legal professionals in the UK published today suggests that the risk of cyberattacks is a growing concern for most law firms, although there is a worrying minority that is still complacent about the risks.

The survey conducted by IRN Research and commissioned by Menlo Security (http://www.menlosecurity.com/), a leader in cloud security, found that respondents are most concerned about the impact to a company's reputation as a result of a cyberattack, with 92% admitting it could be damaging or very damaging. There are also concerns about a firm's inability to continue operating (90%) and the risk of data loss (87%).

According to the survey, more than three-quarters (77%) switched to remote working during the pandemic, and 56% of those are in law firms that have changed or updated their cybersecurity measures to deal with this. Only a minority (45%) of these firms have updated their cybersecurity training to address new ways of working, leaving possible gaps in employee training and awareness.

In addition, just under half (47%) of firms introduced more digital services for clients during the pandemic. Of those launching additional services, 77% updated their cybersecurity measures as a result. However, only 47% offered additional security training corresponding to the new services.

Worth around £37 billion (https://www.businesswire.com/news/home/20210429005544/en/United-Kingdom-Legal-Services-Market-Report-2021-Reven the UK legal market is an attractive target for cybercriminals due to the large quantities of confidential information, financial documents and highly sensitive client data that law firms handle and process. According to IBM's Cost of a Data Breach Report 2021 (https://www.ibm.com/uk-en/security/data-breach), the average cost worldwide of a data breach for professional services organisations was $4.65 million.

A quarter (26%) of legal professionals work in a law firm that has experienced a cyberattack. A third of these respondents say the attack closed services and operations for a few hours, but nearly one in five (18%) experienced delays of one or more days. The majority of firms (57%) have procedures in place to deal with an attack, leaving a sizeable minority (43%) that are not fully prepared.

Published industry guidance not acted on:

In the last 18 months, both the Solicitors Regulation Authority (SRA) (https://www.sra.org.uk/) and The Law Society (https://www.lawsociety.org.uk/) have published guidance notes on cybersecurity, with advice for law firms on how to develop their policies and procedures accordingly. The SRA also opened a consultation with its law firms to ask for feedback on plans to clarify the scope of cover in professional indemnity policies when a firm is subject to a cyberattack, the results of which were

published last October (https://www.sra.org.uk/globalassets/documents/sra/consultations/combined-responses-pii-cybercrime.pdf?version=4a9ff4).

More than six in 10 (64%) are aware of the SRA guidance and two-thirds aware of the consultation, but only 35% have read the guidance, and 41% the consultation documents. In terms of The Law Society guidance, just over half (54%) are aware of it, but only a third have actually read it.

“It’s interesting to see how different industry sectors manage security threats,” comments Mike East, VP Sales EMEA at Menlo Security. “We expect the legal profession to be prepared and well organised to deal with cyberattacks, given the extremely sensitive nature of their work and the fact that increasingly, legal documents are being created, collaborated on, and shared online.

“What’s clear is that the transition to new ways of working – and the fact that legal professionals are often dealing with multiple parties – makes them a serious, and often easy, target for cyber criminals. Menlo Security recently highlighted the growth in HEAT (Highly Evasive Adaptive Threats) attacks, largely a result of hybrid and remote working with employees spending much of their working day in the browser accessing cloud applications. HEAT techniques are often used by attackers to bypass a company’s traditional network security solutions and infiltrate networks.”

He adds: “While the legal industry is taking action to address the challenges with guidance and advice, it’s concerning that more are not acting on it. At the very least, law firms should be updating their policies and procedures, training staff, and looking at gaps in their security stack to address the potential risks of remote and hybrid working.”

Additional survey findings:

- Almost three-quarters (74%) of respondents see phishing emails to clients as either “threats” or “significant threats” to the legal services sector overall, while 60% give a similar threat level for these phishing emails when it comes to their own law firm.

- In general, cybersecurity issues are seen as more of a threat to the legal services sector overall compared to their own law firm. The exception is mobile phone-related security threats, with 60% seeing these as “threats” or “significant threats” in their own law firm compared to 54% for the legal services sector overall.

- Ransomware and malware on websites are seen as less of a threat for the legal services sector by a third of respondents. Malware on websites and ransomware are considered even less of a threat to specific law firms – 37% and 35% respectively.
More than a third (37%) suggest that their firm’s cybersecurity measures have had an impact on their productivity, but around half (51%) feel that there has been no impact.

- One third of respondents feel “responsible” for identifying and reporting a cyber threat while 28% feel “very responsible”. Almost 1 in 5 (19%) believe it is not their responsibility to identify and report these threats.

- Just over half (52%) work in a firm where there is a dedicated person to deal with cybersecurity, but in 38% of firms, there is no dedicated resource.

To read the full UK Legal Services Cybersecurity report:
https://info.menlosecurity.com/rs/281-OWV-899/images/IRN-Menlo-Cybersecurity-Legal-Research%20Report-May-22.pdf

Survey methodology
In March 2022, IRN Research was commissioned by Menlo Security to undertake independent research amongst 150 legal professionals in the UK. Using an online survey, professionals were asked questions relating to cybersecurity in their own law firm and in the legal services sector in general. The survey sample consisted of legal professionals primarily in UK law firms with an annual turnover of between £10m and over £100m including 22 firms from the UK Top 100. A small sub-sample included 15 in-house legal professionals.

About Menlo Security
Menlo Security protects organisations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security's isolation-powered cloud security platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies, eight of the ten largest global financial services institutions, and large governmental institutions. Menlo Security is backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Mountain View, California. For more information, please visit www.menlosecurity.com.

About IRN Research
IRN Research (trading name of IRN Consultants Ltd) is a full-service market research consultancy with a strong track record in providing market research and analysis services to the legal services sector. Clients include law firms, other legal services providers, regulators, and a range of suppliers to the legal sector. If your needs are for a small-scale UK-based research project or for a large- scale, multi-country research project, we can help. We use a range of market research techniques, including desk research, telephone/ online surveys, face-to-face interviews, focus groups, and can provide a full results analysis. Responding to our client's needs, we go beyond the data and present our clients with actionable insight. We also publish a range of annual market reports on the UK legal sector providing a unique resource for monitoring trends in the sector.

PR contact:
Amanda Hassall, Origin Comms
amanda@origincomms.com
T: +44 (0) 7855 359889