National Cyber Security Centre (NCSC) updates advice for Legal Firms

How securing your communications channels can help

LONDON, UNITED KINGDOM, July 24, 2023 /EINPresswire.com/ -- The National Cyber Security Centre has recently updated its Cyber Threat Report for the UK Legal Sector. Last published in 2018 the report gives a summary of what's changed during the intervening years, to help firms understand current cyber security threats, and the extent to which the legal sector is being targeted. It also offers practical guidance on how organisations can be more resilient to these threats.

> There is no doubt that the legal sector is experiencing increasing threat levels from cyber criminals"
>
> *David Holman, Director, Armour Comms*

SRA finds 75% of legal firms reported a cyber attack
The Solicitors Regulation Authority (SRA) stated in September 2020 that 75% (30) of the firms that they visited while researching for the report had been the target of a cyber attack. https://www.sra.org.uk/sra/research-publications/cyber-security/ In another 10 cases, clients of firms were targeted directly during a financial transaction.

Serious impacts for clients and reputational damage
There is no doubt that the legal sector is experiencing increasing threat levels from cyber criminals. This is understandable given that firms are typically handling sensitive client information, for example, relating to criminal cases, or mergers and acquisitions, or handling large financial transactions. Cyber attacks and the compromise of data can have significant implications for clients, not to mention damage to the reputation of a law firm. Indeed, NCSC warns that larger organisations are even being targeted by nation states if they are working on causes with which the state disagrees, for example, human rights or regime change. Some firms have suffered intellectual property theft from state sponsored actors attributed to China. Similarly, firms working in life sciences or energy sectors are seeing increased attacks from hacktivists.

However, it doesn't end with nation states and organised crime. NCSC also warns that there is a growing threat from 'hackers-for-hire' who can be commissioned to carry out malicious activities for people or organisations prepared to pay. This typically involves industrial espionage, and theft of sensitive information that could give an advantage in a legal case and seriously impact your client, for example.

The NCSC report outlines the main types of cyber attacks which include:

- Phishing
- Business email compromise (BEC)
- Ransomware and other malware
- Password attacks
- Supply chain attacks

And gives advice on the best way to tackle each.

A common theme – communications channels

Social engineering – the insider threat

A theme common across all of these attack vectors is the insider threat – i.e. the ability for people to be manipulated by clever social engineering during routine communications, whether this be voice calls, emails, instant messaging or video/conferencing calls. Several of the attacks listed above trick people into actions that can result in malware or other forms of cyber attack infiltrating the business.

BYOD – risk to business data

In addition, if people are using their personal devices (BYOD) for business communications this can open up the firm to additional risks such as compliance and GDPR contraventions, as well as issues around data sovereignty and separating business and personal data on unmanaged devices.

Identity spoofing

Another common theme is that people are tricked into revealing confidential or commercially sensitive information in the mistaken belief that they are communicating with someone they think they know. In other words, identities are hacked or spoofed, either as part of a deepfake scam or business email compromise (BEC).

Secure and compliant collaboration

The answer is to provide secure collaboration tools that are easy and intuitive enough for everyday use. Tools that are designed with security in mind from the ground up (with settings which automatically default to a secure configuration without any intervention from the end user) are a crucial part of protecting employees from social engineering attacks, and keeping sensitive client information, and financial transactions, safe.

Providing a secure communications channel can add an extra layer of security to address the risks for when the stakes are high, providing cyber and operational resilience. Large financial

transactions, details of on-going criminal cases, mergers and acquisitions, sensitive client information all benefit from the additional security that a Secure-by-Design communications solution can provide. Using closed-group communications platforms where only known, previously approved users can get access can dramatically reduce the likelihood of phishing, deepfake or BEC attacks.

Such solutions must also provide Archive and Auditing features, so that details of communications are preserved, and available for review at a later date (subject to strict security measures), even if the conversations/documents have been deleted or lost from the original device – thus satisfying legal compliance requirements, public records needs, freedom of information (FOIA), etc.

Securing Communications Channels Buyer's Guide
Armour Comms has recently published our Securing Communications Channels Buyer's Guide. It provides the Top 10 Questions to ask when Securing your Communications and explains:

- Why and when you need secure communications.
- Are consumer apps secure enough? (No, they are not!)
- Who got caught out?
- What exactly you should be looking for

Download your copy here.

David Holman, Director, Armour Communications.

Andreina West
Andmar
+44 1491 281297
email us here
