LOCKTON AFFINITY LAWYER

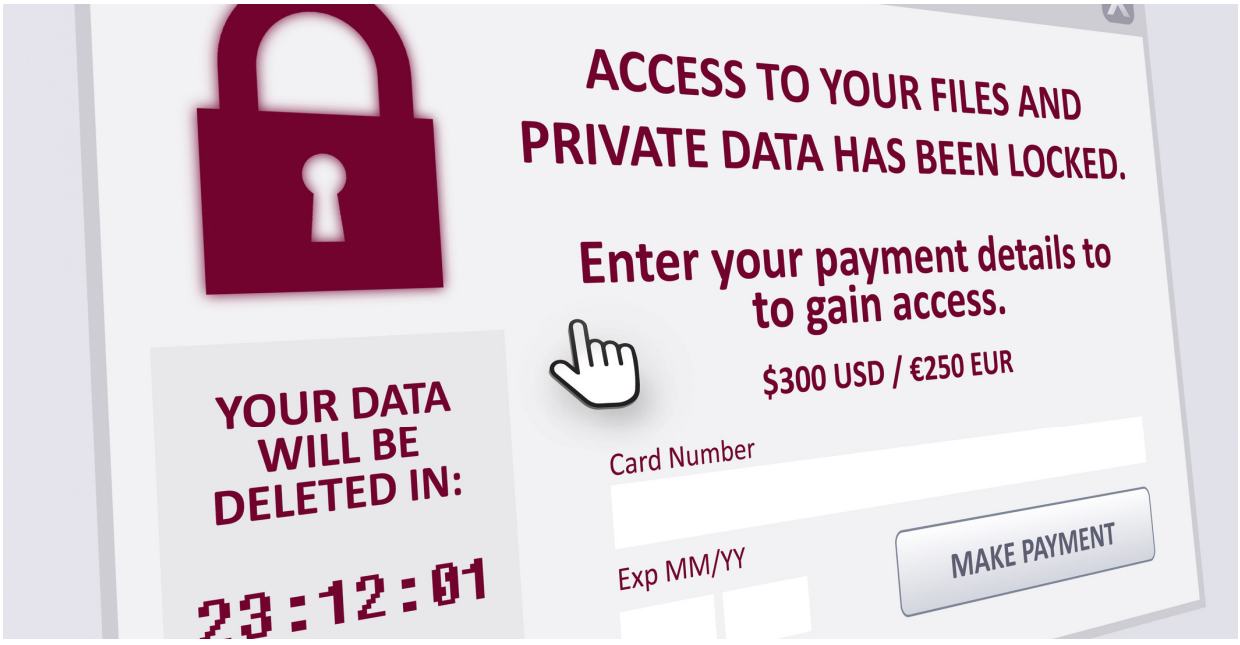
Increased Ransomware Attacks Targeting Law Firms

News about the outbreak and spread of Covid-19 dominated headlines in 2020. Yet for many law firms, Covid-19 has not been the only kind of virus threatening their businesses.

In the past year, there has been a massive surge in ransomware attacks targeting law firms, costing law firms hundreds of millions of dollars, exposing sensitive client data and crippling their ability to operate.

Many law firms continue to focus primarily on their client matters, not realizing how a ransomware attack could now devastate their own practice.

Here's what you need to know about the increased ransomware attacks targeting law firms and what to do about it:



Cyber Crime and Covid-19

The Covid-19 pandemic has played a large role in the current ransomware surge. Criminal enterprises are thriving, as bad actors take advantage of new vulnerabilities created by the pandemic. These tricks abuse users' social trust as well as technical systems.

In several cases, hackers have been caught sending malicious emails disguised as informational messages related to Covid-19. More and more email recipients are opening these messages, clicking on dangerous links, and getting tricked into downloading software viruses.

While most users know not to click on suspicious links, these messages can look official. Many are disguised as email forwards from the World Health Organization.

New technical vulnerabilities are also having an impact. Many lawyers are working remotely, using unprotected home networks instead of their professionally secured office networks.

A ransomware attack that might be stopped by the office network has a higher chance of getting through on a lawyer's personal home network, due to the difference in security settings.

Ransomware Attacks Explained

Successfully recognizing and preventing a ransomware cyber-attack really comes down to lawyers understanding the nature of the threat. To understand ransomware, remember an attack has three aspects:

- **Your files become inaccessible.** When the type of software virus or malware called ransomware infects your computer or network system, the program encrypts your files, such as documents, spreadsheets and PDFs, so that they cannot be opened or edited.
- **A ransom is demanded.** After files are encrypted, a message is displayed on the screen instructing the user to send a payment to release the data and decrypt it. Ransom demands can vary from a few hundreds of dollars to tens of millions.
- **Your data may be exposed.** With recent ransomware attacks, such as REvil and MAZE, hackers also steal a copy of the encrypted data, often threatening to publish it to compel victims to pay the ransom.

Ransomware attacks can be devastating for law firms due to the sensitive nature of the work and the data involved. Both large and small firms are at high risk.

- In May, one of the largest entertainment law firms in the country, Grubman Shire Meiselas & Sacks, was shuttered by a REvil ransomware attack that stole the firm's data. The hackers then leaked 2.4 gigabytes of data related to one of Grubman's famous client's, the singer Lady Gaga, when a ransom of $21 million was not paid.
- In January, a two-partner law firm in Oregon was the victim of a MAZE ransomware attack that encrypted and stole firm data with threats to publish it. With the firm's practice areas including family law, juvenile law and criminal defense, exposure of stolen data could be very damaging to the firm and its clients.

Ransomware Attack Prevention

Ransomware attacks are often a numbers game. Hackers mass-distribute their malware and wait for an unlucky law firm to take the bait and make a mistake. You can minimize your firm's risk of experiencing a ransomware attack with the right steps.

- **Train your employees.** Help your employees learn how to recognize suspicious phishing emails and safely report them to your firm's network security administrator.
- **Back up systems securely.** Be conscientious about testing and storing data backups. Make sure to keep a backup offline that isn't vulnerable to ransomware infections.
- **Practice good patch management.** Adopt software patch management practices to protect you from software vulnerabilities. Consider investing in real-time patching.
- **Implement multifactor authentication.** Requiring multifactor authentication for access to computer systems can reduce the risk of unauthorized access and malware infection.
- **Scan and filter content.** Activate security features to scan and filter email and web content. Your security system can alert your administrator if a problem is detected.
- **Monitor network activity.** Always ensure your network administrator has systems in place to monitor your network for any unusual events or user activity.
- **Limit employee access.** Control access to protect your employees and your data. Limit employee access only to the computers and networks essential to their work.
- **Create an incident response plan.** Have a plan of what steps to take and what personnel to contact in the event of a network intrusion. Train employees on the plan.

If you suspect your computer or network is suffering from a ransomware attack, act quickly. Take a picture of any screen messages and contact your network administrator right away. Disconnect the computer from the network, pulling the plug if necessary. Avoid rebooting or restarting your machine.

These tips can help your firm lower your risk of a cyber attack, but even the best security precautions can't prevent all attacks. Take the next step by protecting your law practice with cyber liability insurance from CyberLock Defense.

Discover more benefits of professional liability and cyber insurance for your firm today at Lockton Affinity Lawyer or (844) 398-0465

Information provided by Lockton Affinity is not intended as legal advice.