The weakest link

How to work remotely in a cyber-safe environment

INTERVIEWED BY JAYNE GEST

PAUL SEMS
Chief technology officer
Blue Technologies Inc.

(216) 271-4800
psems@btohio.com

WEBSITE: To learn more about Blue Technologies Smart Solutions' Legal and Professional Services team, visit www.btohio.com/industry-experience/legal-professional-services.

When it comes to cybersecurity, you're as strong as your weakest link — and that often comes when your employees work offsite. This is true for many industries, and it's undoubtedly important for law firms or corporate legal departments where reputation is critical.

In the Panama Papers leak, more than 11.5 million documents from Mossack Fonseca described over 200,000 shell corporations used for tax evasion. In 2016, three foreign nationals hacked into a New York City law firm to use information for insider trading, gaining more than $4 million.

"The risk associated with law firms is higher as they become a bigger target. You can easily find examples of firms that have been compromised and all of their client data has been made public. The threat is real," says Paul Sems, chief technology officer, Blue Technologies Inc.

Lawyers Mutual reported 22 percent of law firms experienced a cyberattack or data breach in 2017, which was up 14 percent.

Smart Business spoke with Sems about how to ensure cybersecurity is part of the equation when legal professionals work remotely.

Why is working remotely a security concern?

Most organizations, including law firms, have systems to ensure the on-site network is secure. The real challenge comes when employees want to bring their devices into your network or work remotely. They may use a home computer with viruses on it, or their computer-provided laptop doesn't have the same firewalls and intrusion detection when it's using public Wi-Fi. You're going into an unknown or uncontrolled environment where 1) you could be susceptible to additional threats, and 2) your information could be intercepted.

What can ensure remote access is secure?

You need to implement the following:

- **Education** — Train anyone who uses technology systems. They need to be aware of social engineering attacks and educated on what they should and shouldn't click. They need to understand which wireless networks are safe. For example, don't connect to free Wi-Fi. Instead, bring a hot spot or sync to your phone. The Webroot Threat Report's 2018 midyear update found companies that ran one to five security awareness training campaigns saw a 33 percent phishing click-through rate. That drops to 28 percent with six to ten campaigns and 13 percent with 11 or more campaigns.
- **A properly configured environment** — Have your IT professional ensure your system is compliant with best practices, such as correct and secure settings for phones, laptops and the accompanying software, and that devices are up-to-date.

  Data needs to be stored securely. In most cases, attorneys can access all client data. That data, however, needs to be encrypted by default, which is also called encrypted at rest, so it's not easy for just anyone to read those files. This needs to occur both within the office and with remote access — in case someone loses a laptop or a device is compromised. The encryption needs to be set up for transport so that no one can listen to the communication. All law firms should encrypt email, which is now available on all the modern platforms, including Microsoft.
- **Continuous monitoring and remediation** — Keep an eye on your systems to ensure they still are compliant. Then, not only are you detecting the problem, but you're also getting help to get it fixed.

How can technology providers help?

An outside provider can do initial security assessments and ensure the management system is tracking everything in a secure environment, both on-premises and through remote access. It also can help provide a response plan so you know how to respond to an incident. Moreover, it can monitor and maintain that environment, in the event the internal IT staff is busy on other matters.

Legal and professional services have unique challenges and therefore may need specialized solutions. For example, if attorneys have international clients, they fall under the new General Data Protection Regulation in the European Union. It is data protection by design and by default, which means you have to run a secure infrastructure and if someone compromises data you have significantly increased liabilities. Make sure your technology provider has experience in your industry to truly understand its nuances. ●