Published on *The National Law Review* https://natlawreview.com

How Lawyers Should Handle Thumb Drives

Article By:

Cyber Liability, Data Security and Privacy at Raymond Law Group LLC

As part of investigations and discovery practice, lawyers regularly request and receive electronically stored information. This may be through a FOIA request, or from medical records requests, or prior counsel's files, or subpoenae duces tecum, or Rule 34 requests, or directly from a client. ESI may be provided on a CD or DVD, or a thumb/flash/usb drive, or an external hard drive, or through a third-party cloud host. Unfortunately, this practice is replete with risks.

As recently reported, in a police whistleblower case in Arkansas, the plaintiffs' counsel received from opposing counsel, an external hard drive containing request document and...four Trojans. Many attorneys, paralegals, and other legal support staff might not think twice about inserting a disk or device received from a known third party into their computer. Fortunately for the plaintiffs' counsel here, he thought better of it. Had he not done so, it is possible that the firm's entire computer records could have been transmitted to a data thief or the firm could have been locked out of its files.

If physical file transfer creates risk of infection, cloud systems present their own risks. Dropbox and other cloud systems can be hacked or create opportunities for employees to easily steal information. Unencrypted data can be accessed by the cloud system and delivered to third parties.

With that in mind, lawyers and law firm managers need to consider these risks as part of their ethical duties. Among potential solutions are: lock-out computers to preclude use of a USB drive; review the terms of service of the cloud storage provider; strongly encrypt all confidential files on the firm's computers before sharing with a cloud provider; and use an unconnected computer to scan all third-party media before it reaches the firm's network.

Although this matter affects all types of businesses, law firms are especially vulnerable due to the information collection and distribution requirements of practice. The firm's network IT is not necessarily going to be an expert in data security. Facing liability for a data breach and a bar complaint arising from the same oversight must be considered.

National Law Review, Volume V, Number 110