LegalInk
magazine

IS YOUR LAW FIRM'S MOBILE DATA REALLY SECURE?

Law firm IT departments face the challenge of keeping data secure as more and more lawyers and legal teams use their mobile devices to work remotely. The benefits to having remote access to confidential information from anywhere are obvious, but firms also need to know what to look for to keep their information (and their clients' data) safe from deliberate and accidental breaches.

In order to keep data secure, IT departments need to understand what their firms' risks are, what app functionality is required to ensure data is secure and the policies they need to implement for attorneys and staff.

The Evolution of Technology and Work Habits

Ten to fifteen years ago, attorneys who wanted to access information while away from their office had few options. IT departments would provide the best choices they could, which still required attorneys to carry a bulky laptop computer with a modem connection that would have to be plugged into a telephone jack. The speed would have been minimal, as would the usefulness of the data.

In the intervening years, the dramatic improvements in cell phone data capabilities, the development of smartphones and the overall consumerization of technology have led to practically every professional having the ability to access any information they desire, whenever they want and wherever they might be. This hasn't just impacted IT professionals by creating the expectation that information from the work environment can be accessed 24/7; clients also expect to be able to access their data whenever they want, and they expect their attorneys to be responsive whenever they have questions.

While there are many advantages to increased mobility, there are also dire consequences when law firms fail to keep data safe. Even major law firms struggle with issues of data security and breaches. In March, The Wall Street Journal reported that some of the nation's largest law firms, including Weil Gotshal & Manges and Cravath, Swaine & Moore, had been breached by hackers. While the extent of the breach wasn't clear, the Manhattan U.S. attorney's office and Federal Bureau of Investigation had become involved.

The leak of the so-called “Panama Papers” has also put the issue of law firm data security under a microscope. In that incident, more than 11 million documents, many of them highly sensitive, were stolen from the Panamanian law firm Mossack Fonseca.

In this environment, it is imperative for law firm IT departments to create strong data security policies, choose the right technologies and provide the right training. Clients demand it, and law firms have an ethical and professional obligation to provide it.

Keeping Data Safe

Keeping mobile data secure requires a three-prong approach: technology, processes and training.

Technology: Law firm IT departments can adopt several best practices around technology to vastly increase data security. Installing a firewall on an internet connection is one of the most basic steps firms can take to keep data secure. Since lawyers and staff are connected to the internet, and the internet is connected to them, information can flow freely both ways. Firewalls act as sentry and gatekeeper to prevent unauthorized access to computers and networks.

IT departments also need to use encrypted servers that are thoroughly protected. Firms should also provide encryption for all sensitive files and provide training on the importance of using it.

Outsourcing security operations center (SOC) services is another step to consider. Today it is rare for firms to utilize an SOC that can analyze all incoming traffic and determine if it is malicious, benign or questionable. If the SOC identifies code that is malicious in nature, the provider should have steps in place to repair any and all damage.

Processes: IT departments need to implement processes to augment their technology. That includes presenting a strong and mature methodology for information security and breach prevention by having plans for virus protection and monitoring email gateway and web and firewall configuration. The firm should also have a contingency plan to assess and monitor vendor security.

Law firms should identify a team to take charge of server maintenance and security measures.

It is beneficial for the firm to create and consume internal and external threat intelligence. By participating in the sharing of information, a firm may be able to benefit from such practices and galvanize security toward threats through education and knowledge of these factors.

Firms should also create a support policy that covers responses to lost devices. Considering the potential for data being exposed when a phone or tablet is lost or stolen, IT departments need to implement a process for reporting these types of situations and then remotely wiping them. This policy should also be enacted when lawyers and staff leave the firm.

In order to keep data safe, firms should have a policy that requires attorneys and staff to use an encrypted data network at all times to protect sensitive data, as well as policies that utilize technology like two-factor authentication, other domain authentication practices and configuration profiles.

Training: Aside from all the technological methods of data breaches, the most common areas of vulnerability are actually human-related. Law firms should create a culture that demonstrates their institutional commitment to protecting client data and present that engagement and commitment to all staff, from IT to junior and senior members.

As part of that commitment, firms need to train all users on the importance of encrypting sensitive data. While encrypting data can be cumbersome, it is a necessary step. This is particularly true when attorneys use mobile devices. While attorneys may be tempted to respond to a short email while they are waiting at the airport or stopping for a cup of coffee, public networks are generally not secure. That means that a quick email may leave client information vulnerable to an accidental or deliberate data breach.

Many of the benefits of mobile devices—their small size and easy transportability—are also what makes them so easy to steal and lose. Unfortunately, no level of malware, antivirus and firewall security can prevent an ingenuous individual with the right knowledge from accessing all personal and sensitive information from devices. This is why developing the right technology, processes and training is so important. With these in place, firms can minimize the risk that information will be accessed by the wrong individuals.

About the Author

Philip Homburger is the president of LawBase. He was the initial programmer of LawBase 36 years ago and has been instrumental in its growth into one of the leading case and matter management solutions on the market today.

Originally published July 25, 2016 by Legal Ink Magazine, http://legalinkmagazine.com