Is Emailing Confidential Information a Safe Practice for Attorneys?

BY MARK LANTERMAN

As technology becomes increasingly complicated and integrated into how we communicate, the rules governing its use must adapt accordingly. Attorneys are held to several ethical and legal obligations when it comes to protecting their clients' data. Most notably, Colorado Rule of Professional Conduct 1.6(c) states that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Because this data is often communicated via email and through the Internet, those within the legal community are held to the highest standards of cybersecurity and discretion when it comes to handling data breaches and cyber events. Unfortunately, though, some attorneys seem to believe that the word "reasonable" allows for a fairly low standard.

The Problem with Email Disclaimers

In my experience, the majority of lawyers depends on the confidentiality statement in their email messages to protect them from data breaches or errant emails. Many have confidentiality notices that read something like: "The information contained in this electronic transmission (including attachments) may contain confidential information. If you are not the intended recipient, please contact the sender and destroy all copies of this communication." This seems like enough, right? We're only human after all, and other methods like encryption or secure portals seem cumbersome.

That line of thinking is absolutely wrong. Attorneys are strongly obligated to protect their clients' data, and email disclaimers actually do very little, if anything, to protect the data contained in email communications. At best, they are a feeble attempt to shift blame from the errant sender to the unwilling accidental recipient. They do nothing for the clients whose information is compromised, and they often jumble together "confidential" and "privileged" as interchangeable notions. Confidentiality is an ethical duty that has an extensive reach, protecting all information relating to client representation; attorney–client privilege protects client–lawyer communications for the sake of representation and may not be protected if the information is available from another source. Notably, information that is protected under confidentiality requirements may not be protected under attorney–client privilege. Disclaimers may have a small role in ensuring safe delivery when an email actually contains confidential or privileged information, but in terms of protecting client data, they are not useful, especially when they come at the end of an email instead of the beginning.

In addition to email, most attorneys take advantage of easy and effective communication via portable devices such as smartphones and laptops on a daily basis. This makes cybersecurity considerations much more complicated. When data is leaving the physical confines of the office, attorneys need to consider all of the potential vulnerabilities that may affect their devices, including the physical risk of theft.

Encryption Techniques

Encryption is an easy way to mitigate this risk and account for the expanding network of devices that a law firm stores client data on. Encryption is way to protect data by essentially making data unreadable until it is unlocked with a "key" via a process known as decryption. Encryption is a valuable tool for protecting data that is stored on an "at rest" system (e.g., an external server) and data that is sent via email or through the Internet.

It is important that encryption policies be standardized within a law firm. Manufacturer instructions for full-disk encryption, operating systems encryption, and encryption software must be followed for best results. Because data loss is a possibility if decryption keys are lost, backups are important and centralized controls should be implemented to control and manage encrypted data.

For data that is being transmitted, wireless networks must be actively secured. For devices used outside of the protected office network, it is important that attorneys do not use unprotected public Wi-Fi or networks for transmitting confidential information via the Internet. Those within the legal community have an ethical obligation to verify that the networks they connect to are secure; because this is nearly impossible in a public space, refraining from working in these environments is ideal.

Attorneys have the utmost responsibility to protect client data. With this in mind, encryption for email should be an option in appropriate circumstances. When an email is marked as being confidential or privileged, the best method is to secure the email or relevant attachment with encryption. Keys should be sent separately. Most critically, attorneys should be clear with clients about what types of information will or will not be transmitted via email. This is not only for the purposes of confidentiality, but also for the sake of avoiding phishing scams or other email-related cybersecurity events.

Most critically, attorneys should be clear with clients about what types of information will or will not be transmitted via email. This is not only for the purposes of confidentiality, but also for the sake of avoiding phishing scams or other email-related cybersecurity events.

As an alternative to email, there are secure portals that allow for secure and easy messaging with clients without the same hassle as email. Within these already encrypted environments, attorneys can communicate with clients efficiently. In my estimation, the most daunting part of this is convincing your clients to refrain from emailing you directly and communicating solely through the portal.

Great Expectations

With cybersecurity breaches affecting law firms, new expectations surround what is required of the legal community in protecting their data. As in the healthcare sector, attorneys have to take security measures that are equal to the importance of the data with which they are entrusted. A primary tool in this effort is to communicate to clients what exactly will be communicated digitally and how that communication will be managed in the most secure way possible. CL

Mark Lanterman is chief technology officer of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, he has 28 years of security/forensic experience and has testified in over 2,000 trials—mlanterman@compforensics.com.