Swiss Re
Corporate Solutions

Ten tips for law firms to avoid a cyber incident that threatens client confidentiality

Lawyers and law firms are vulnerable to cyber incidents

Unfortunately, law firms are still regarded as "soft" in the comparative world of cyber targets. Many law firms use systems that are easier to hack than those of their more sophisticated clients. This imbalance in technology leaves the law firm as the weakest link in the data chain and an obvious target for cyber criminals.

Further, even if lawyers are employed at firms with sophisticated systems, they are still vulnerable to social engineering attacks as well as to simple mistakes. Lawyers must work efficiently while looking for new opportunities as well as assisting and procuring potential clients. Consequently, many lawyers will click the links contained in unsolicited emails, fall for phishing scams, or simply make mistakes during the course of email exchanges.

Competence and confidentiality

In addition to a financial and a practical problem for lawyers, a cyber incident may lead to ethical problems as well. The ABA Model Rules make clear that it is no longer acceptable for a lawyer to simply claim technological ignorance. What follows is a reminder of how the ABA Model Rules speak to technology:

- ABA Model Rule 1.1: Competence, Comment [8]
  "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice ***including the benefits and risks associated with relevant technology,*** *engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."*

- ABA Model Rule 1.6, Confidentiality
  "(c) 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." See also, Comment [18] and [19]

No lawyer wants to be the subject of a grievance or law suit as a consequence of technological incompetence and/or the failure to protect confidential client information. The following tips may assist in that regard.

Ten Tips for maintaining confidentiality in the cyber world

1) Train your entire team All attorneys, staff, and vendors must exercise the utmost level of cybersecurity care, awareness and diligence. Training in cyber breach prevention and mitigation should be mandatory for *everyone* in every law firm, from the founding partners to the receptionist. Remember- you are only as strong as your weakest link. Employing and/or training a technologically proficient team is the best prevention to a cyber incident.

2) Train to curtail human error The majority of all security incidents are caused by human error. Consequently, the most sophisticated security system in the world is irrelevant if the potential for human error is not addressed. For example, one law firm with a strong security system discovered someone had accessed client files. After performing numerous systems checks, the law firm ultimately discovered that an employee kept her passwords on a notepad in her unlocked desk drawer. A member of the cleaning staff found the notepad and was able to access client files.

Further, many law firm partners still send confidential information from personal email accounts, use public Wi-Fi systems while waiting for flights or having coffee, and take other risks, such as failing to password protect their smartphones. Training and enforcement of cyber policies for *everyone* in the firm is necessary to avoid these common human errors that can lead to cyber breaches.

3) Send fake emails To further provide cyber security training, a number of corporations and large firms now routinely send fake phishing emails to test their employees' cybersecurity awareness and to determine the number of employees who open the emails. These corporations then advise their employees of the open rate percentage and instruct them regarding the red flags that were ignored. For example, employees may ignore a change in the sender's email address protocol, fail to hover over a link before clicking it (the name displayed may indicate that the link is not as represented), and may ignore other information that would indicate that the email is a fraud. Feedback has been found to be effective in encouraging employees to exercise more care in opening the next link.

4) **Pause before sending text messages and emails** The "reply to all' key has been responsible for confidentiality breaches, embarrassment and awkwardness. Further, accidentally sending to the wrong "Mary" or not realizing that the actual plaintiff has been copied on a document can cause further problems. Disabling the "reply to all" button and pausing an extra second before pushing "send" is obviously good practice. There are also options to color code emails so that "outside" vs. "inside" emails are easily ascertainable.

Further, avoiding the text message in a professional setting is perhaps the best course. While a text may be an acceptable way to communicate with friends and family, it is not the ideal form of communication for use in a professional setting due to its fast and informal nature, and the potential that it will not be saved to the file.

5) **Encrypt** Encryption is thought to be the least used security feature found in most law firms. While encryption of *all* files is currently not ethically mandated, the failure to encrypt could arguably be viewed as a breach depending upon the circumstances. ABA Model Rule 1.6 reads:

> ...This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. Comment [19]

Lawyers should therefore evaluate the security needs of the actual data for each engagement to make certain that the confidentiality needs of their clients are adequately protected. Obtaining the client's written and informed consent and advising them of potential confidentiality issues, before using email or text messaging to communicate with them, is also advisable.

6) **The cloud** While many attorneys conceptually understand that information stored in a cloud is stored off site, many are unaware that depending upon the vendor, cloud data could be stored internationally, governed by foreign law, and subject to search and seizure. Further, if an attorney places data in the cloud that is subject to state or federal privacy laws, the client should first provide their informed and written consent for such storage (adding this item to the engagement letter may be an option). Finally, the attorney should check with the bar association for their respective state's ethical opinions that govern cloud storage.

7) **Update your systems** Law firms should update their systems, including the VPN, antivirus, anti-spyware and spam filters routinely. Do not delay when a system advises that an update is warranted. Outdated systems often times contain open doors for hackers to walk through and infiltrate.

8) **Vet vendors** Vendors have been identified as the weak link in certain large exposure hacking incidents. Recall that in some recent attacks, hackers were able to access the security systems by stealing credentials from a vendor. Examine all vendors' cyber security protocols (does the vendor encrypt data and/or use a VPN system?) as well as the vendor's insurance policy and all controlling contracts. Understand where the vendor will store the information – international storage may present problems. Examine indemnification clauses and provisions regarding who will be expected to pay in the event of a data breach.

9) **Have a plan** Every law firm should establish a plan to follow in the event of a cyber breach. Further, like fire drills, law firms should practice cyber drills. Are documents routinely backed up? Are copies of the most important documents at an off-site, secure location? In the event of a hack or a ransom, does everyone know who to call? Vendors should be selected ahead of time so that in an emergency, the law firm is not panicked and scrambling. For example, privacy counsel, to establish immediate privilege and provide notice requirement advice, can easily be researched ahead of time. Selecting or creating a list of professionals to assist with restoring data or handling a ransomware incident should also be researched. Finally, cyber liability coverage can help in this regard. Cyber insurance, in addition to covering the costs related to a data breach, such as notification expense and regulatory fines, can also provide professionals to assist in case of an emergency to help develop a plan.

10) **Passwords** Law firms should encourage strong passwords. The password should contain letters, both upper and lower case, characters, and numbers. One idea is to anchor your password to a phrase instead of a word. For example "She Loves to travel to Warm Weather and go swimming" can translate to the following password by using just the first letter of every word, with capitalization every so often: SLtttWWags. The value to this new password is that it is very hard to guess without knowing the original sentence, but yet easy to remember. Adding numbers and characters will then create a stronger password. Another option is to use a secure password generator.

In conclusion, law firms continue to be soft targets for cyber hackers. Following these tips may serve to help prevent a cyber incident, and may assist in more quickly responding to such a situation should it occur.