RHODE ISLAND
Lawyers Weekly

Volume 42 • Number 50 • December 13, 2021

SPECIAL FEATURE:

Avoiding a fire drill: insurance dictates and law firm cybersecurity protocols

By Don Nokes

Law firms in today's marketplace are facing a slew of cybersecurity mandates from their insurers and, in some cases, their business partners (banks, credit card processors and other large vendors), given the proliferation of hackers and breaches.

In fact, we've seen evolving policy requirements and firms dealing with the immediate need to implement increased cybersecurity safety protocols — in a fire-drill mode - prior to renewal of their policies.

As a result, law firms are well advised to proactively cover their bases. Basically, we tell law firms that just because they have met the criteria for their current policy, they shouldn't be lulled into thinking their renewal will require the same levels of cyber safety.

For example, as our clients have been renewing their cybersecurity insurance policies, they are discovering security strategies that were once optional are now mandatory to keep or purchase new coverage. What's it's common for firms to learn of more stringent renewal requirements close to the actual policy termination date.

Don Nokes is the president and co-founder of NetCenergy, a regional IT support firm that specializes in securing professional services firms.

Beyond the technical safeguards, we know that implementing best practices include protecting law firms' systems and data, guarding against damage to law firms' reputation, and, ultimately, minimizing the law firm's liability.

For those who have experienced a hack, they know breach notifications alone are enough to paralyze a law firm for several weeks.

MFA: necessary security protocol or nuisance?

The most common new requirement that we're seeing is Multi-Factor Authentication or MFA. When it comes to MFA, law firms are finding they will need to attest that MFA is invoked at every level and for every user. Carriers are now placing this attestation as a new condition for renewal.

MFA grants access when the user combines something they know, such as a password, with something they have, typically a cellphone or an email account. When the user attempts to login, the software will require the usual password but will then prompt the user for a code that is delivered via text message to the registered user's cellphone or email account.

MFA implementation can create operational challenges, although not in cost or implementation time.

In addition to your technical support team, a comprehensive rollout of MFA involves every user with access to your network. This requires buy-in from everyone at every level at your firm and an executable plan that aims for little or no disruption to major deals, complex litigation, and the day-to-day activity of running a business.

We see the best results when MFA is introduced over several weeks.

Tips for an MFA program roll-out in- clude alerting your users in advance, probably via email, and providing some video or in-person training to those unfamiliar with MFA. The process will need to be added for each software program that your users access.

Beyond MFA

MFA is the most common new requirement we are seeing, but it isn't the only one. Other best practices for law firms include regular security awareness training, ethical phishing, implementing a disaster plan, and encrypting data during transit and/or while stored on the firm's electronic file system.

• Security awareness training

Various cybersecurity experts estimate that as many as 93 percent of all successful breaches begin with email.

Most firms have deployed effective email filtering solutions designed to warn a user if an email message seems amiss. These tools will typically err on the side of caution and may quarantine a legitimate email message. Other times the tools may caution the user about opening the message, but if the user opens it anyway, the technical safeguards are, in effect, disabled and the breach can proceed.

This is why cyber insurance carriers want to know how often your users are being exposed to security-awareness training. This specific training has two goals: to provide users with the skills to identify the telltale signs of a phishing email and to keep security top of mind.

More often than not, the user who causes a breach will acknowledge that they thought the message seemed a little off. They may offer excuses about a busy workload, a looming deadline or court date, and/or fear of disappointing the partner in charge with a work slowdown if they stopped to verify the validity of the email.

Our advice for law firm leaders is to insist on regular participation by your entire user community. Your firm may be at risk for a denied daim if the insurer can show that you are not complying with the attestations you made regarding frequency of training.

• Ethical phishing

Many users can't identify a harmful phishing email. The time to learn is during a controlled initiative and not when they receive a phishing email during a busy or stressful day.

For law firm users at all levels, we recommend that your outsourced or internal IT team initiate an "ethical" phishing test at least once a quarter.

In this model, your users will receive an email they should be able to identify as a phishing attempt. Your security team should use strategies such as staggering the dates and times that the emails are sent and altering the subject and details of the phishing requests so that users aren't tipped off. The process is logged, and the results are discussed with the users who were duped into taking action.

Obviously, there is significant value in identifying the users who require more training.

• Disaster planning

Best practices dictate that every law firm has an up-to-date disaster planning policy and procedures guide for when a disaster strikes. With this guide, you can invoke your response in a methodical and timely way and, ultimately, reduce the time it takes to get your systems back online and your users resuming productivity.

Once your policies and procedures have been set, it's vital you your entire staff in the event of an emergency.

We recommend your guide include: factors that need to be met before declaring an emergency, a plan to notify users of the issue, how to determine when and if specific vendors should be brought in to assist, and communication to the appropriate users, stakeholders, clients and others that that there is an emergency.

A well-thought-out disaster plan will likely be a new requirement imposed by the insurance carrier on law firms, regardless of firm size.

• Encrypting data in transit and/or at rest

Data encryption was popularized after the National Bureau of Standards created the Data Encryption Standard, or DES, in 1977 and still serves as an effective and popular method.

Current standards for law firms include data encryption for sending and receiving sensitive information (to clients, courts and adverse parties), but your carrier may also require encryption for "data at rest" or when your data is stored on your on-site or cloud-based data storage system.

In summary, we see a lot of activity from cyber insurance carriers. They are looking to reduce their own exposure by requiring increased security for their insureds through tools and methods to protect against and avoid costly breaches. The result is that more law firms are implementing the full menu of best practices to protect themselves.

If you are fortunate enough to have es-caped a hack or breach, there are three possibilities: You have enacted these best practices, you have just been lucky, or maybe your systems have already been compromised without your knowledge.

Regardless, between the increased incidence of hacking and the added pressure applied by liability insurance carriers, now is a good time to review your practices before they are mandated. **RILW**