10 Security Questions Managing Partners Need to Ask Their IT Directors

by Sharon D. Nelson and John W. Simek

Too often, law firm managing partners are content to let their IT departments operate on cruise control — until a crisis strikes. There are so many questions that they should be asking that it was hard to winnow our list down to ten.

1. How do we ensure that we are installing all critical updates and patches for our software and hardware? Believe it or not, this is the number one reason for data breaches — the failure to patch. There should be a reporting mechanism so that you receive weekly reports of all updates made — you don't have to read it, but at least there will be an audit trail — and making the report will constantly remind your IT director to be vigilant.

2. How often do we require passwords to be changed and what are our rules for password strength? Today, sadly, the answer should be every thirty days (no repeats) twelve characters, using upper and lower case, numbers, and special characters.

3. How are we preparing to move beyond passwords? Passwords will be obsolete in the near future. Google is already moving to two-factor authentication and has announced that it will move away from "passwords only" in the future. Biometrics is one option, but we prefer two-factor authentication using some kind of token (something you physically have) in addition to a password (which now doesn't have to be as complicated).

4. What is our process for securing data when we terminate employees? There should be a checklist of items to go through, including the return of all data, killing IDs and the ability to connect remotely, retrieving all firm cell phones, laptops, prox cards, keys, etc. If they have a personal code to get in the office, terminate the code. The list is long.

5. Do we change the defaults on all our equipment? This is the second most common reason for breaches — defaults are unchanged on routers, etc. and even the script kiddies (never mind the true cybercriminals) know all the defaults. There should be reports verifying this as well.

6. What is our incident response plan? If you suffer a breach, is there a team in place? Who needs to be notified? Do you have a digital forensics company that you can call to investigate and remediate a breach? Do you have an attorney who is a data breach specialist who can assist in helping you comply with any federal or state notification laws and regulations? Another long list here.

7. Do we have redundant hot and cold backups and a plan for business continuity in the event of an emergency?

8. Do we have a Bring Your Own Device (BYOD) policy? If so, have we recently evaluated the risks of having personal devices connected to our network?

9. Are we storing data in the cloud? If so, make sure that a lawyer has actually read the terms of service and your IT director has adequately investigated the cloud for physical and data security — including whether the provider will advise you of any law enforcement requests for your data in time for you to file a motion to quash. No notice will be given if the requests are under the Patriot Act, but most of them are not.

10. How are we protecting mobile data? Do all laptops have full disk encryption? Do we have adequate remote access policies? When attorneys connect remotely, is the data encrypted in transit?

There could be 100 questions — easily — but start with these ten to get a handle on how well you are securing your law firm data!

Nelson

Simek

Sharon D. Nelson and **John W. Simek** are the president and vice president, respectively, of Sensei Enterprises Inc., a digital forensics, information security, and information technology firm based in Fairfax. Nelson is president of the Virginia State Bar.