Bloomberg BNA | ABA

ABA/BNA
Lawyers' Manual on Professional Conduct™

Confidentiality

A Primer on Cyber Damages and How to Avoid Them

By Melissa M. Lessell

Although many lawyers, especially those at smaller firms, think that they could not be a target for a data breach, they're dead wrong.

So said panelists Sharon Nelson, president of Sensei Enterprises Inc. and immediate past president of the Virginia Bar Association, Robin Campbell, senior counsel and co-chair of the Privacy and Security Group at Crowell & Morning in Washington, D.C., and John Simek, vice president of Sensei Enterprises, who spoke at the ABA Standing Committee on Lawyers' Professional Liability's Spring 2015 National Legal Malpractice Conference in Washington.

Campbell said ''one of the problems with law firms is that people are reluctant to acknowledge that they have personal information.'' Campbell also explained that the decentralized law firm structure makes it harder to identify sensitive data and risks.

Cyber Breaches Are on the Rise

The numbers don't lie—the reported incidents of data breaches are rapidly increasing, up 20 percent from 2013 to 2014.

However, the number of records exposed as a result of data breaches actually decreased by 7.1 percent, though Nelson said she believes this number will likely increase in 2015 due to the large scale breaches of January 2015.

The number one sector for data breaches is health care, with the annual cost associated for breaches estimated to be $5.6 billion. Even a small breach can cost hundreds of thousands of dollars, which can consist of paying fines to regulators and employing best practices such as credit monitoring, to protect those whose personal information was inadvertently disclosed.

The largest number of breaches occurred in California, followed by New York, Texas and Georgia. And of course, these numbers only relate to reported breaches. Many do not get reported, especially by law firms because they are ''worried about feet running for the door,'' Nelson stated.

The FBI issued an alert in 2009 warning that law firms were at-risk targets of future data breaches. In 2011, the FBI met with the 200 largest law firms to discuss their respective security and data breach policies.

According to Mandiant, a company believed to handle the largest number of law firm data breach investigations, approximately 10 percent of its work comes from law firm breaches, handling 80 law firm breaches in 2010 alone.

Nelson said the perpetrators of data breaches have ''changed dramatically over the years.'' She told the attendees that, in 2014, 60 percent of data breaches were performed by cyber criminals, over 20 percent from state-sponsored espionage and only 7-8 percent by ''insiders'' such as a disgruntled employee.

Defining and Responding to a Breach

The panel defined ''privacy'' to be ''protecting individually identifiable information.'' However, Campbell noted that each state seems to define what constitutes identifiable information differently.

The state leading in privacy-related class actions due to favorable laws—California—defines identifiable information to be merely name and e-mail addresses. Forty-six states and the District of Columbia have data breach laws.

Although many of the breach and third-party spying stories seem remote in a traditional law firm setting, the panel pointed to real-life examples, including two Wilson Sonsini breaches which were used to further insider trading, and a breach of Wiley Rein in 2012 by Chinese hackers who went by the name the Byzantine Candor.

Melissa Lessell is a partner in the New Orleans office of Deutsch, Kerrigan & Stiles LLP, where she represents lawyers, accountants, agents and other professionals in litigation and disciplinary proceedings.

 ISSN 0740-4050

The Byzantine Candor also targeted the EU Council, Halliburton and 18 other groups in July 2012.

Simek noted that small firms are vulnerable to breaches as well. Small and solo law firms are targeted when third parties are looking for such things as health care data and credit card information, which many small firms store in spades.

Further, data controlled by a law firm's human resources department are often confidential, highly sensitive and a potential target for a security breach.

E-mails hosted by a website provider are also a possible point of vulnerability. The panel noted that screensaver sites are one of the most notorious sources of malware, along with pornography sites. Firm-wide institutionalized blocking of such sites minimizes the potential for unauthorized access.

Campbell advocated that law firms conduct a risk assessment to determine the firm's subjective weaknesses and vulnerabilities. It is recommended that the firm appoint a privacy officer who creates a security plan in conjunction with the firm's general counsel, human resources, public relations and information technology departments.

The point of the plan is to have a ''well defined approach,'' detailing what constitutes an incident, when an incident is triggered and when it needs to be escalated.

Campbell also recommends that the plan be given a test run to identify any potential gaps or points of confusion.

In the case of an actual security breach, Campbell recommends bringing lawyers in early to establish privilege, since almost every step taken is done in anticipation of litigation.

Law firms are notoriously behind their clients in terms of security policies. Some major clients require firms to certify that data they provide to the firm are secure, either via a third-party security audit or a self-certification procedure. ''Training is one of the most surefire ways to avoid problems with cyber security,'' she said.

Protecting a Law Firm's Information

The speakers said one of the most common, but preventable, law firm security failures is not applying security patches or other updates. Law firm leaders must affirmatively confirm that the IT department is regularly updating the software used.

Nelson also cautioned that firms should not use Microsoft XP or Microsoft Service 2003 as they are out of support, meaning new updates and security patches are not made for them for newly discovered threats. If a program is out of support, ''we must, must, must change the software,'' she said.

Nelson said that because of the security risks associated with these programs, ''it is flatly unethical to use [them],'' but that many firms do for budgetary reasons.

The discussion also included technology law firms use and how to make sure the most secure method is employed:

Encryption

Nelson identified encryption as one of the most essential tools law firms must employ to secure data. Encryption was defined as a ''secret language'' analogous to keeping a document in Klingon (a fictional language spoken by the Klingons from Star Trek).

All devices should be encrypted and, if possible, should be encrypted at the hardware level. Simek recommended using enterprise encryption if more than one computer is being used, using such products as Symantec Encryption or Sophos SafeGuard-Enterprise Level. Windows EFS should not be used.

On personal computers, encryption can be deployed through using Bit Locker on Windows-based operating systems, or File Vault on Macs.

Sensitive e-mails should also be encrypted. Sensei uses ZixCorp to encrypt e-mail, a program that integrates with Microsoft Outlook.

Smartphones

''Every one of your smartphones has confidential data on it, even if you don't mean there to be,'' Simek warned.

Although no smartphone is secure out of the box, the panelists identified the Blackphone by Silent Circle as the most secure; the Department of Defense uses it.

After the Blackphone, Androids and BlackBerries are the most secure phones, in terms of possible security. iPhones are the fourth best option, though widely used.

Regardless of what type of smartphone is used by lawyers in a firm, the data should be encrypted. Simek explained how easy it is to employ encryption on smartphones. To employ encryption on an iPhone, the owner simply has to enter a password. With an Android, a box has to be checked in settings which encrypts all data on the phone.

Cell phones can also have anti-malware programs installed; these programs include Lookout, Kaspersky and McAfee.

Simek also said law firms should require all smartphones connected to the network to have passcodes and auto-timeout features enabled.

In addition, firms should be able to remotely wipe all data from the phones. As a best practice, Simek explained that firms should not allow employees to use their own devices on a firm network, unless the firm has mobile device management software.

Cloud Computing

More than 50 percent of lawyers are using cloud computing despite the fact that the cloud may be breached. Nelson noted that cloud computing is really just outsourcing from an ethical point of view, so the same ethics rules would apply.

The panel was quick to disabuse those in attendance of the notion that platforms such as Dropbox are secure. Since Dropbox holds the master encryption key, if required to do so by subpoena or law enforcement action it has the ability to turn over the data uploaded without notice to the law firm.

Rather than using this type of platform for cloud-based storage, the panelists advocated using a platform with ''zero knowledge,'' meaning that the user retains the master and only encryption key. If a zero knowledge platform tried to access the data—even if responding to subpoena or law enforcement agencies—the information would not be useful or comprehensible.

The panel also stressed the importance of determining up-front how a law firm will be able to retrieve its data at the conclusion of the contractual relationship

  MOPC ISSN 0740-4050

with the cloud storage facility or if the company were to go bankrupt.

In addition to Dropbox, commonly used programs such as iCloud, Google Drive and One Drive use a master encryption key. To safely use those programs, it is recommended that the data be encrypted before it is uploaded.

SpiderOak, on the other hand, is a natively zero knowledge cloud storage system. Interestingly enough, the journalists who had Edward Snowden's data stored it in SpiderOak. Box is currently beta testing a user controlled encryption platform that likely will be released in the summer to consumers. (As of now, Box is not a zero-knowledge cloud storage system.)

WiFi Access

There are three methods of encryption for wireless devices. The only secure wireless connection is WPA2. WEP or WPA are not secure connections. Apple products cannot determine the encryption of the WiFi network until after the device has been connected to it, so it is important to verify if the network is secure before using an Apple product on wireless Internet.

On the other hand, Simek said ''anything that uses a cellular data network is reasonably safe'' as the data stream itself is encrypted.

Passwords

A secure password is essential. To be secure, a password should be at least 14 characters and include numbers, letters and special characters. If a password manager is needed, the panel recommended E-Wallet.