Bloomberg BNA

ABA/BNA Lawyers' Manual
on Professional Conduct, Current Reports™

Source: ABA/BNA Lawyers' Manual on Professional Conduct: News Archive > 2013 > 08/28/2013 > Conference Report: ABA Annual Meeting > Confidentiality: Firms Must Keep Watch Against Hacking And Other Intrusions on Confidential Data

29 Law. Man. Prof. Conduct 555

Confidentiality

Firms Must Keep Watch Against Hacking And Other Intrusions on Confidential Data

SAN FRANCISCO —"Hundreds of law firms are being targeted by hackers," said panelist John Simek at "Locked Down: Safeguarding Client Information," presented by the ABA Law Practice Management Section during the ABA Annual Meeting here on Aug. 8.

Simek is vice president of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm in Fairfax, Va.

A recent ABA survey found that 23.9 percent of responding lawyers from firms with 10 to 49 members had had some sort of security breach, panelist David Ries noted. Ries is a partner with Clark Hill Thorp Reed, LLP, in the firm's Pittsburgh office.

Perhaps even more frightening, Ries said, "25 percent of respondents answered 'we don't know' if we've ever had a security breach."

And when they do, "It's usually around eight months before a law firm discovers it's been hacked," Simek added.

Unwanted Attraction

Law firms have become an increasingly attractive target for hackers because lawyers need "to know everything about their clients" and therefore compile a great deal of sensitive information in electronic form, Simek said. At the same time, he commented, law firm partners "often want all sorts of privileges," including administrative rights and the freedom to transfer documents to their mobile devices.

Citing the ABA survey and a study from the information security company Mandiant showing increasing attacks on and breaches of law firm security, Simek said it is crucial for law firms to understand where risks of information breaches exist and what they can do to minimize those risks and comply with their ethical obligations.

One law firm, Ries said, was notified by the FBI that the law enforcement agency had encountered all of the firm's client files on a server overseas that was known to transmit information to China. Other law firms, too, have been successfully hacked by Chinese entities or shadowy organizations such as hacker collective Anonymous, he said. And, illustrating the power of an individual's low-tech human error, the panelists noted that a Maryland law firm lost unencrypted patient medical data when a staffer left a USB drive on public transportation.

"A computer lets you make more mistakes faster than any invention in human history—with the possible exceptions of handguns and tequila," one speaker said, referring to a quip in a magazine article quoted in *United States v. Carelock*, 459 F.3d 437, 443 (3d Cir. 2006).

"Our number one duty to our clients is confidentiality," Ries said. That duty, he noted, arises from several sources: the rules of professional conduct, common law, contracts that an increasing number of clients require their law firms to sign, and statutes and regulations, including the Health Insurance Portability and Accountability Act (HIPAA).

Rule Amendments

Ries noted that the August 2012 amendments to the Model Rules of Professional Conduct included adding language to the Comment to Model Rule 1.1 to specify that the duty of competence requires lawyers to keep apprised of "the benefits and risks associated with relevant technology."

He also pointed out that Model Rule 1.6(c) goes beyond protecting only the "confidences and secrets" of clients, as DR 4-101 of the Model Code of Professional Responsibility did, and requires "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

Comment [18] to Rule 1.6 specifies factors for determining whether protective efforts are reasonable. As an example of what would be a beyond-reasonable effort to prevent unauthorized access by hackers, Ries offered a "50-character complex password." It "costs nothing, but that would make it impossible to use technology," he said.

In the Air, Out the Door

There are a number of ways in which information can leave a firm, the panelists said, including thumb drives and file-sharing applications such as Dropbox. Data may also be sent to a Web-based e-mail address, Simek noted, in which case the only evidence will be on the employee's computer.

For securing those avenues, Simek said, "Consider securing your USB ports or logging all activity" on firm computers. "You can install software on a computer to find out when a flash drive is inserted, its manufacturer, and the serial number of the flash drive," he explained.

"Fifty-nine percent of departing employees acknowledge that they take data," Simek said. "Make them sign a statement on exit" that they have not retained any client data and have returned any data in their possession, and that they understand that taking or retaining information that they are not authorized to possess is a crime, he recommended.

Software exists that can crack a four-character iPhone password in 15 minutes.

John Simek
Sensei Enterprises, Inc.

Additional safeguards that the panelists recommended include keeping all applications and operating systems up to date and minimizing the number of partners or employees with administrator privileges. White-listing applications, meaning "telling a computer that these are the only applications it may run," is another excellent security precaution, Ries said, as are removing any unneeded services and enforcing strong passwords.

Simek said eight-character passwords, which not so long ago were considered sufficient, can now be cracked in two hours or less. Twelve-character passwords, on the other hand, which are now generally recommended, currently require 17 years to crack, he said. And those four-character default passwords on your smartphones? Simek said "Software is specially made to crack a four-character iPhone password in 15 minutes." Ries advised: "Use as many [characters] as you can live with."

Other best practices Simek offered included mixing upper- and lowercase letters, numbers and symbols, using passphrases, refraining from using passwords or PINs for more than one task and changing them regularly.

Lost or Tossed

Simek also cautioned the audience to dispose of hardware securely. "Two-thirds of computers [bought and sold on eBay] have recoverable data," he said. He recommended using software, some of which is freely available, to wipe data from a computer before disposal, but cautioned "If you have two hard drives, take out the one you don't want wiped!"

Among professionals, lawyers are the heaviest users of smartphones, the panelists said. Because smartphones are often lost or stolen, "You need to be able to remotely wipe" it in case of loss or theft, Simek said.

Limiting confidential data on a smartphone, setting an automatic logoff after a certain time, locking or wiping after a set number of failed logon attempts and refraining from installing apps that want access to your contacts are also good security measures, Ries added. "Pay attention to the permissions," he said. Additionally, "Be careful when using public and unknown wireless clouds, or avoid using them," Simek said.

Encryption, Simek said, will go a long way toward protecting data and, added Ries, "It's really easy to have a tech person set it up." He said "Encryption is really scary to attorneys. But once it's on, you don't even see it. It's seamless."

In addition to the risks applicable to desktop computers, mobile devices are subject to danger from scanning QR codes that send the device to a site that will install malware, said Ries. "Bad guys stick them on restaurant menus" posted outside establishments, Simek stated.

The panelists illustrated the ease with which surreptitious hacking can be accomplished by demonstrating the capabilities of the WiFi Pineapple Mark IV, a security-testing (and hacking) device available for less than $100. Because the device "can hijack your connection by impersonating remembered networks," Simek said, it is important both to turn off your device's WiFi connection when you're not using it and to tell the device to forget a network once you're finished using it.

Anonymous Attention

Similar warnings and precautions punctuated a program on "Cyber Nightmares in the Law Office—Why Law Firms and General Counsels Must Care: Firsthand Experiences in Handling (and Surviving) Data Security Attacks," presented Aug. 10 by the ABA Section of Science and Technology Law.

The discussion was moderated by David Z. Bodenheimer, a partner in Crowell & Moring LLP's Washington, D.C., office.

Panelist Rich McClain described firsthand his firm's experience as the target of a cyberattack by Anonymous in late 2010 and early 2011. McClain is information technology director in the Richmond, Va., office of Hunton & Williams LLP.

"WikiLeaks announced they were going to publish a trove of Big Bank confidential information. Big Bank engaged Hunton & Williams to help research the possible data breach and manage or mitigate its liability," McClain said. The law firm began forming teams to assist its client, including technical experts and experts on banking in

addition to its legal team. The teams held meetings, "documented the situation, made recommendations, and sent lots of e-mails with summaries" of meetings, opinions, and recommendations.

In that process, "a boutique security firm tried to join the party and help." That company "devised a plan to supposedly destroy WikiLeaks. They proposed their plan to various key players with no success." Then, McClain said, the security company "decided to tout their plan in the international press, so it then became very public information."

Unsurprisingly, he said, "WikiLeaks and Anonymous heard about the plan and decided they needed a copy. Within 24 hours, Anonymous breached the boutique security firm and stole the plan, along with thousands of e-mails and a Facebook site."

Other players mentioned in the e-mails then became its targets, McClain said—including the law firm. "It became an attack on us when it appeared that countermeasures were being considered to not only thwart but also impair the attacker," i.e., Anonymous.

Lessons Learned

McClain said his firm learned a number of lessons from the attack.

In addition to basic safeguards such as "strong and diverse passwords, updated firewalls and patches," he advised lawyers to "Know where your information is," store it offline, and "Build strong relationships between your legal and technical professionals," starting before your firm ever experiences an attack.

"People, including lawyers, are the weak link."

Cheryl Falvey
Crowell & Moring LLP

McClain also cautioned "Be careful what you put in e-mails," whether or not they're encrypted. "Recognize that no organization is immune or impenetrable," he said. "There's nothing like a direct attack. It's not like a pedestrian consumer-grade malware."

Greetings From China

Panelist Cheryl Falvey described the challenges of the federal Consumer Product Safety Commission in dealing with "a systematic and state-sponsored exploitation of the commission's website over quite a long period of time." Falvey, now a partner in the Washington office of Crowell & Moring LLP, was general counsel for the CPSC from 2008-2012.

Falvey said "Before I joined the commission, it had already been hacked by the Chinese," as she had learned when she represented a client before the agency "and was told to hand-deliver my client's design documents instead of e-mailing them."

But "Whether we liked it or not," Falvey said, "the Chinese government that was potentially behind the exploitation of our systems was also our business partner. We had to work with them" on issues involving problems with China-manufactured drywall used in U.S. homes.

The delicacy of the situation, and the importance of human interactions as the first line of cybersecurity defense, came into focus, she said, when experts arrived from China to share their drywall knowledge with the CPSC.

"The Chinese took out a USB drive to begin their PowerPoint presentation. We had so trained our workforce about not using USB drives that it was as if they had taken out a gun," she said. "We took an early lunch and gave it to our IT department to scan it and make sure we could use it."

Lead by Example

Falvey emphasized that when it comes to cybersecurity, "People, including lawyers, are the weak link." Observing "It's really hard to take a BlackBerry away from a lawyer," she said general counsels "must lead by example" to show that no employee is above the rules.

For Falvey, leadership "meant I had to take the yearly training [in security] or have my access cut off." Agreeing with McClain that relationships are paramount, she said that back in the private sector, "It helps to have strong relationships with government investigators before you're hacked."

"As [financial institutions] become harder ... to hit, there has been an increase in attacks on law firms. That's where the information is."

Former FBI Agent Mary Galligan

Panelist Mary Galligan said cybersecurity "is not an IT issue and not a CIO issue. It has become a CEO, managing partner, president of company issue. If it doesn't start up there, you can have the best IT department and equipment in the world, but you've still got a problem." Galligan, who recently retired after 25 years as an FBI agent, is set to join the New York office of Deloitte & Touche in September as a managing director in its security and privacy practice.

Clients Too Must Be Careful

Galligan warned that law firms may become targets as the results of their clients' actions, as happened at McClain's firm. "Your client made an unpopular decision, so [hacktivists such as Anonymous and LulzSec] are going to come steal your information and embarrass you," she said.

She said corporate espionage is also a problem: "Financial institutions have been hit very hard. As they become harder and harder to hit, there has been an increase in attacks on law firms. That's where the information is." And according to Galligan law firms' cybersecurity is not as strong as it is in other places. "More and more clients are asking about cybersecurity before they hire you," she said.

Galligan said it is particularly important to advise clients to limit access to information to those who need to have it. "Does HR really need the same access as those in financial?" she asked. "Lots of companies give all departments the same level of access."

Another speaker, Peter McLaughlin, said "It's very important that everyone understand that simply because you are a smaller firm or a solo practitioner, you still have information that is very valuable to your clients, whether it's intellectual property, trade secrets, or employment data. Keep in mind that failing to properly protect your client data may subject you to any number of ethical issues." McLaughlin is of counsel in the New York office of Morrison & Foerster LLP.

What's 'Reasonable'?

"The ethical rules say if you apply 'reasonable' security to your systems and client information, then even if it gets lost or stolen, you won't be found to have violated your ethical obligation," McLaughlin said.

But "the standard of reasonable security leaves much room for dispute," as Bodenheimer and Falvey wrote in their article, *Cybersecurity Standards and Risk Assessments for Law Offices: Weighing the Security Risks and Safeguarding Against Cyber Threats*.

The article describes how some law firms have addressed information security concerns and suggests some generally applicable standards. The authors also provide guidance for lawyers to use in formulating policies and procedures for their own offices.

McLaughlin said it is imperative to take to heart Model Rule 1.1's requirement that you understand the benefits and risks associated with technology as part of your duty of competence.

In case of a cyberattack, he said, "Be aware that in addition to dealing with the nightmare of trying to regain control over your systems, and trying to placate the government or clients who are mad as all get-out over losing their data, if you haven't done your homework in advance, then you could well find the additional problem of an ethical complaint."

By Helen W. Gunnarsson

For More Information

The article by Bodenheimer and Falvey on cybersecurity for law offices is available at http://www.americanbar.org/groups/science_technology/pages/2013annualmtgmaterials.html.

ISSN 1521-5083