May, 2016

Cybersecurity Best Practices for Information Professionals

Darla W. Jackson

CYBERSECU

BEST PRACTICES FOR INFORMATION PROFESSIONALS

Tips for creating awareness and best practices for reducing security risks.

BY DARLA W. JACKSON

IN THE PAST FEW YEARS, THERE HAS BEEN CONTINUED TALK ABOUT CYBERSECURITY INCIDENTS. The headlines have been filled with news of the Target security breach and the resultant litigation and congressional hearings, the Sony Entertainment hack, the Home Depot breach, and the breach of the Federal Office of Personnel Management. Cybersecurity has become a major concern for the legal community as well. Although law firms have been, and continue to be, reluctant to report specific incidences of breaches in response to industry surveys, more firms are starting to acknowledge them.

RITY

As reported in the *American Bar Association (ABA) TECHREPORT 2015*, 15 percent of respondents to the *2015 ABA Legal Technology Survey* reported that their firms had experienced a security breach at some point. There has also been coverage of specific breaches and ransomware victims in large and small law firms. On March 30, 2016, *The American Lawyer* reported an incident in which hackers gained access to the networks of law firms working in the mergers and acquisitions (M&A) area. The article detailed a *Crain's Chicago Business* report that confirmed a significant number of firms were targeted by a Russian hacker seeking M&A information. Similarly, an *ABA Journal* Daily News post entitled "Lawyer Resigns Himself to Paying Ransom for Release of Computer Files," reported a small Oklahoma firm's computer files were being "held hostage" as part of a ransomware scheme for the second time in the last few years.

But firms are not the only targets of cybersecurity crimes in the legal community. Legal information vendors, including LexisNexis, have also suffered loss of data. In a 2014 issue of *Business Insurance*, Richard Bortnick described a compromise of a vendor's database that allowed hackers to access an international law firm's servers resulting in hundreds of employees' W-2 forms as well as other information.

Court systems have also been victims of those working to illegally access or block access to data. For example, in January 2014, the *ABA Journal* Daily News confirmed that a group had claimed responsibility for denial of service attacks against the Public Access to Court Electronic Records (PACER). Similarly in 2013, *Forbes Tech* detailed the attack of the Washington State Court system, which resulted in potentially 160,000 social security numbers being accessed.

At the 2014 E-courts Conference, organized by the National Center for State Courts, Bryant Baehr, chief information officer of the Oregon Judicial Department, in a presentation entitled "Cybersecurity: What Judges, Court Administrators, and Court Technologists Must Know," not only acknowledged that courts are targets of cyber-attacks, but also suggested that encryption and two-factor authentication should be utilized to limit the success of such attacks. Despite security measures—such as maintaining backups—denial of service as well as ransomware and data mining attacks continue to grow. For example, according to a post on the Daily Journal website, the Kankakee County Court system in Illinois was "taken hostage by a hacker using ransomware on Feb 26, [2016]." The county refused to pay the ransom, citing the availability of backup files to "rebuild" the system.

> If legal information professionals are not familiar with the details of the security atmosphere that currently exists, they should first concentrate on becoming more aware of the security risk.

University systems supporting professional schools, including law schools, have also increasingly become cyber targets. According to a July 2013 *New York Times* article entitled "Universities Face a Rising Barrage of Cyberattacks," universities throughout the United States are increasingly under attack, with "millions of hacking attempts weekly." In February 2014, the University of Maryland reported that it had been attacked and social security numbers for more than 300,000 individuals had been accessed, and in 2016, *Campus Technology* reported that the University of Central Florida experienced a similar data breach. Further, as universities have begun issuing devices and students continue to insist on using their own devices to conduct educational activities via university networks, security becomes an increasingly important issue. According to a 2013 *EdTech* magazine article, mobile device management is no longer optional for institutions engaged in educating medical professionals in teaching hospitals, which are required to comply with Federal regulations concerning the confidentiality of healthcare information. As law schools increasingly engage in clinical and experiential work—in part to fulfill the requirements for such opportunities set forth in Chapter 3 of ABA's *Accreditation Standards*—academic personnel may find that they also are "required" by ethical considerations, client expectations regarding confidentiality, and perhaps even future enhanced regulation to manage access to information in a manner to ensure greater security.

In these types of environments, and despite assertions that security is "everyone's business," law librarians and legal information professionals have often marginalized security concerns, noting that security is the responsibility of the Information Technology (IT) Department. Instead, librarians are often interested in a "philosophy of freedom" of information with an emphasis on open source products and access, and are frustrated by network or other security concerns that may interfere with open access initiatives. This commitment to open

There is a need to find the right balance between accessibility and security.

access is reflected in the preamble of the 1999 AALL Ethical Principles:

> When individuals have ready access to legal information, they can participate fully in the affairs of their government. By collecting, organizing, preserving, and retrieving legal information, the members of the American Association of Law Libraries enable people to make this ideal of democracy a reality .... [F]ostering the equal participation of diverse people in library services underscores one of our basic tenets, open access to information for all individuals.

However, the commitment to open access should not overshadow all other principles; AALL's Ethical Principles also note that AALL members "uphold a duty to our clientele to develop service policies that respect confidentiality and privacy." Service polices certainly must address access to electronic and digital resources and data, taking into consideration the reasonable steps needed to minimize the risk associated with access in order to protect the confidentiality of users.

Further, as law librarians and other legal information professionals increasingly serve as administrators of both the library and IT functions or as chief information officers, the marginalization of security concerns and the delegation of security as the sole concern of IT can no longer be justified. This is particularly true in cases where there are no or few IT or technical support staff. Even if law librarians are not responsible for the IT function, Jody R. Westby, CEO of Global CyberRisk LLC, notes that there must be a recognition that security "is an enterprise issue, and that means that attorneys, firm management, and support personnel (including legal information professionals) need to be involved."

There are some actions that law librarians might consider taking to assist in reducing security risks. Closing every security loophole and blocking every vector of attack would likely render networks unusable for patrons. Thus, there is a need to find the right balance between accessibility and security. To facilitate conversations about the balance, law librarians and legal information professionals have to become more familiar with the security environment and best practices for dealing with security risks.

If legal information professionals are not familiar with the details of the security atmosphere that currently exists, they should first concentrate on becoming more aware of the security risks. Reviewing texts that address these security concerns, such as the *ABA Cybersecurity Handbook* by Jill Rhodes and Vincent Polley, and *Locked Down: Information Security for Lawyers* by Sharon D. Nelson, David Ries, and John Simek, would be a start. With increasing frequency, ABA Continuing Legal Education (CLE) offerings also include cybersecurity topics. Participating in such CLE courses, both as continuing learners and as presenters, is a means of not only gaining additional knowledge, but raising the profile of law librarians when it comes to dealing with data security and cybersecurity.

It is likely that current awareness efforts will also lead legal information professionals to literature on the developing and evolving best practices designed to minimize cyber risks. The report from the inaugural ALM Legal Intelligence Law Firm Cybersecurity Survey—*Cybersecurity and Law Firms: Ignorance Is Risk*—outlines best practices for law firms in pre-breach and post-breach situations. In addition, this resource sets forth cybersecurity trends that may influence the development of best practices. While the checklist of best practices included in the report focuses on law firm environments, there are practices that are applicable to other environments as well. Due to the limited scope of this article, not all of the best practices outlined can be addressed. As a result, emphasis will be given to best practices applicable in multiple environments prior to a breach.

1 Identifying the Data Crown Jewels and Limiting Access

This guidance is pretty straightforward and follows previous wisdom that professionals hired to help protect valuable and confidential information must do so. However, all information collected may not be useful for the purposes of a firm's representation.

TAKEAWAY: Recognize that certain forms of information may not be useful to law librarians and legal information professionals. In those cases, don't resist the policies that may restrict access to such information. In other situations, a legal information professional may need access to such information to perform competitive intelligence research or accomplish other tasks.

2 Data Access from Different Devices

The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, by Jill D. Rhodes and Vincent I. Polley, indicates that if a law organization selects to permit personal devices on its network, the organization should use mobile device management (MDM) as a "centralized way to manage mobile devices remotely, including the ability to lock or erase a lost device remotely and check its geographic location." There are a number of leaders in the area of MDM products and services, including AirWatch, Good Technology, and MobileIron, but security experts suggest that MDM is the "bare minimum" for organizations that allow staff to use their own devices to access the networks of the organization—a practice often referred to as BYOD. However, use of a particular security technology does not ensure success. As Charles Magliato wrote in *Peer to Peer Magazine*:

> The issue of managing all mobile devices, both user-owned and firm-supplied, is clearly one that extends beyond tracking inventory and basic security. It requires a comprehensive plan that starts at the top with management buy-in to firmwide policies relating to usage, sanctioned apps, access to corporate data, and auditable procedures to protect sensitive client data in the event of stolen devices. Regardless of the technology used, these strategies will be less than successful without a formal process to educate users regarding appropriate use of mobile devices and their responsibility to act in the best interest of the firm and its clients.

TAKEAWAY: Legal information professionals should also be involved in advocating for and selecting security solutions such as mobile device management products and services that meet the needs of their organizations. Additionally, information professionals should be involved in teaching users about the risks of using the devices and their responsibility to do so in a manner that would reasonably be seen as protecting the interests of their clients.

3 Encrypt Sensitive Data

Law enforcement agencies repeatedly requested that Apple provide assistance with gaining access to the San Bernardino gunman's iPhone, suggesting encryption is a strong security measure. However, security professionals view encryption as a basic safeguard. Notwithstanding, the *2015 ABA TECHREPORT* states "use by attorneys of included encryption tools is very low." Respondents to the *2015 ABA Technology* survey reported "an overall use of full drive encryption of only 20 percent (up from 14 percent last year)…."

TAKEAWAY: Law librarians and legal information professionals may be involved in providing educational support regarding encryption. Many attorneys are not familiar with file, folder, or full drive encryption and may not know the pros and cons of the various encryption techniques. Good communication skills and technology competencies often make legal information professionals excellent candidates for educational leadership roles.

4 Implement Good Password Hygiene

Password development and storage are areas that are relatively simple. At a 2014 CLE program at the ABA's Annual Meeting, Andrew Perlman—a professor and director of the Institute on Law Practice Technology and Innovation at Suffolk University—indicated that "lawyers don't have to be technology experts but should know how to develop strong passwords that will be difficult to compromise." Perlman described a strong password as containing "at least 12 characters … mixing letters, numerals, and special characters, with at least one capitalized letter. Your cat's name, your birthdate or a password such as 123, are not strong…." While some may argue that the use of a strong password on its own is not as secure as a biometric measure or security tokens that provide two-factor authentication, for now, strong passwords remain the most commonly used tool, mostly because they are not as complex to implement.

TAKEAWAY: Legal information professionals can assist others by recommending password generation tools such as Telepathwords, which tests the strength of passwords. Also, because strong passwords may be more difficult to remember, legal information professionals may want to be familiar with password managers, such as LastPast, to assist with password retention. However, the June 2015 breach of LastPast reminds us that these vendors are not immune to cybersecurity concerns.

5 Train and Retrain on Cyber Policies

Many professionals in the area of security indicate that education is perhaps the most important step; in part, because individual firm employees are a primary source of information leakage. Law firms seem to be getting the message. Eighty-seven percent of respondents to the inaugural *ALM Legal Intelligence Law Firm Cybersecurity* survey indicated that they "train employees on processes and polices to prevent data breaches. Training employees on topics such as the effective use of passwords or the recognition of phishing schemes can be low-cost investments that have a substantial return by preventing breaches from occurring at all." However, retraining—particularly in the area of what to do in case of an actual breach—may not occur on a regular basis.

TAKEAWAY: As stated above, because law librarians and legal information professionals generally have good communication and technology skills, they are often called upon to serve as leaders of education initiatives. Despite other work requirements, a commitment to leading training regarding cybersecurity policies is a valuable contribution.

6 Ensure Third-Party Vendors Comply with Security Policies

Third-party vendors should be vetted for cybersecurity practices. Vendors with access to confidential data should also be subject to audits by the company.

TAKEAWAY: Many of the legal information providers with whom law librarians negotiate and work with will not need access to confidential data. Regardless, if law firm personnel will be using network assets to access legal information, the provider should be vetted. Law librarians may be the most knowledgeable about the providers and the details of the negotiated agreement with the vendor. As such, law librarians should be involved in the vetting of these third-party vendors.

Images © iStock.com/JayZynism

7 Use Existing Frameworks and Tools

The National Institute of Standards and Technology (NIST), a part of the Department of Commerce, has developed "a 'cybersecurity framework' to help regulators and industry participants identify and mitigate cyber risks that could potentially affect national and economic security." The framework, adaptable to a variety of organizational structures and organizations, can be used to conduct a basic review of cybersecurity practices, establish or improve cybersecurity using the steps outlined in the framework, communicate cybersecurity requirements with stakeholders, and identify opportunities to revise or create new standards or practices. In June 2013, NIST also released a revision of its *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* As summarized by the Information Law Group, these new guidelines recommend that organizations should:

- Have a mobile device security policy that defines the types of devices permitted, the resources that may be accessed, and how provisioning is handled.
- Develop system threat models for mobile devices and the resources that are accessed through mobile devices.
- Consider the merits of each provided security service, and determine which services are needed for the specific environment and then design and acquire one or more solutions that collectively provide the necessary security services.
- Implement and test a pilot of their mobile device solution before putting the solution into production.
- Fully secure each organization-issued mobile device before allowing a user to access it.
- Regularly maintain mobile device security.

Certainly law librarians could and should be involved in assisting in steps such as developing models for reducing potential threats regarding how legal resources are accessed, as recommended by these guidelines.

TAKEAWAY: Law librarians might advocate for a compromise of positions that allow for a balance between convenience and a need to reduce risk. For example, law librarians could advocate for an information structure encouraging e-books to be downloaded over a secure network and thus accessible on mobile devices, rather than having mobile device users access such resources over insecure wireless networks. Such programs would likely be appreciated by users who have capped data plans on their wireless devices.

8 Purchase Cyber Liability Insurance

Only 70 percent of the respondents to the inaugural *ALM Legal Intelligence Law Firm Cybersecurity* survey reported having purchased cyber liability insurance. However, this is significantly higher than the percentage of *2015 ABA Technology* survey respondents who indicated they have insurance. According to the *2015 ABA TECHREPORT,* the "percentage of attorneys reporting that they have cyber coverage is small: 11 percent overall. It gradually increases from 10 percent for solos to only 15 percent for firms of 500+." Further, experts caution that many firms that have purchased insurance have done so without understanding the requirements and exemptions of their policies. For example, as Laurence Colletti and Sharon Nelson—who spoke at the 2016 ABA TECHSHOW on passing security audits—explain in their Legal Tech Network podcast, some policies exempt coverage of state-sponsored actions, which in many circumstances would exempt coverage of acts initiated in China. Listen to the podcast at bit.ly/MJ16LTN.

TAKEAWAY: Certainly law librarians are well qualified to conduct research on how courts have interpreted specific language in cyber liability policies, and can locate reviews and satisfaction information regarding insurance providers. Get more information about *Cybersecurity and Law Firms: Ignorance Is Risk* at bit.ly/MJ16ALM.

The Law Librarian's Role

With new technological advancements comes new opportunities, threats, and security solutions. No longer can legal information professionals delegate all security responsibilities to IT staff. Legal information professionals need to be aware of the security environment and need to participate in organizational security policy development, security product/service selection, and security educational efforts. Since law librarians are involved in knowledge management and document preservation, they may be highly contributing members of the cyber-attack response teams. If we creatively find opportunities to assist with issues of organization cybersecurity, law librarians and information professionals can add immeasurable value to their organizations. ■

LEARN MORE

Learn more about AALL's Ethical Principles at bit.ly/AALLethics.

AALL 2016 ALERT

Don't miss Darla Jackson and Avery Le's session "Information Security: Changing Access Concerns and Data Protection Best (and Sometimes Easy) Practices," Sunday, July 17 from 11:30 a.m. to 12:30 p.m. For more information visit bit.ly/AALL16InfoSecurity.

© 2016 BY DARLA W. JACKSON

DARLA W. JACKSON
PRACTICE MANAGEMENT ADVISOR
Oklahoma Bar Association
Oklahoma City, OK
darlaj@okbar.org