Thinking About Technology - Cybersecurity: Breaches and Heartbleed to BYOD—Are Bankers, Entertainment Company Executives, Celebrities, Postal Workers, Ice Cream Lovers, Home Builders, and CIOs the Only Ones Who Should Be Concerned?

Darla W. Jackson, University of South Dakota School of Law
Thinking About Technology . . .

Cybersecurity: Breaches and Heartbleed to BYOD—
Are Bankers, Entertainment Company Executives,
Celebrities, Postal Workers, Ice Cream Lovers,
Home Builders, and CIOs the Only Ones
Who Should Be Concerned?*

Darla W. Jackson**

In 2013 and 2014, several high-profile data security breaches underscored the importance of cybersecurity in today’s world, including the legal community. Reports of leaked information and security breaches at legal information vendors, firms, universities, and even courts continue to increase. Ms. Jackson addresses these concerns and suggests some considerations in developing responses to such security threats.

¶1 October 2014 was designated as National Cybersecurity Awareness Month.1 Most individuals, however, did not need such a formal observance to remind them of the increasing concerns regarding cybersecurity. In the past few years, we have continually heard about cybersecurity incidents. During the holiday season of 2013 and into 2014, the Target security breach was in the news. Later information regarding breaches of other service providers’ and retailers’ security led some to designate 2013 as the “Year of the Mega Breach”2 and instigated congressional hearings on the matter.3

¶2 Despite the broad scope of breaches in 2013, the magnitude of the threat in 2014 surpassed that of the previous year. In late November 2014, a hack of Sony Entertainment’s systems resulted in the public disclosure of the company’s internal e-mails, financial information, and information about upcoming movies.4 In October 2014, the Department of Homeland Security released a bulletin on Black-
Energy malware, which was attributed to a Russian hacking campaign against the nation’s critical infrastructure, ongoing since 2011.\(^5\) Earlier in October 2014, news surfaced of a hack of J.P. Morgan Chase that compromised contact data from 76 million households.\(^6\) Dairy Queen also reported that the payment system in 395 of its restaurants had been hacked.\(^7\) In mid-September 2014, the U.S. Postal Service discovered a breach of its systems that “potentially compromised” the personal data of 800,000 past and present postal workers.\(^8\) In late August 2014 and again a few weeks later, “intimate photos” of celebrities obtained without their permission were posted to websites.\(^9\) The celebrity photo incidents were followed by the revelation that lax data security management at Home Depot had allowed a breach resulting in the compromise of credit card information of 56 million customers.\(^10\)

These recent examples are part of a continuous string of incidents involving online security breaches.\(^11\) In addition, the Heartbleed bug and vulnerabilities found in Dropbox also brought the topic of cybersecurity to the forefront.

\(^3\) Cybersecurity has become a major concern for the legal community as well. Reports of leaked information and security breaches at law firms continue to increase.\(^12\) Legal information vendors, court systems, and universities’ systems supporting law schools have also increasingly become cybertargets. Yet a number of technology surveys indicate that many attorneys have little security training or

---


understanding of the security measures undertaken by their firms and organizations. This article addresses these increasing cybersecurity concerns and suggests some considerations for law librarians and the organizations they serve when developing measures to address security threats.

¶ 4 At the 2014 American Bar Association (ABA) Techshow, cybersecurity was a topic of concern for many attendees. Events since 2012 have caused an increased emphasis on cybersecurity. In fact, eighty-seven percent of the technology directors and chief technology officers responding to the 2013 American Lawyer Law Tech Survey indicated that they were “more concerned” about security threats in 2013 than they were two years before. This is not surprising given reports that more firms are being attacked, sometimes without knowing it.

¶ 5 Products and services used by firms were found to have vulnerabilities as well. News of Dropbox’s vulnerabilities to Heartbleed, a bug in the Open SSL encryption code “that could have allowed people to see what was supposed to be encrypted data passing between users and the websites using OpenSSL,” potentially threatened law firms’ data security. Further, Dropbox issues regarding shared links to documents permitting inadvertent disclosure to unintended recipients, although eventually fixed, caused legal technology professionals to advise firms and corporate counsel to block the use of document-sharing tools such as Dropbox.

¶ 6 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. Compromise of a vendor’s database in March 2014 allowed hackers access to an international law firm’s servers, resulting in the breach of hundreds of employees’ W-2s and other information. Court systems have also been victims of those

13. Throughout this article, “law librarians” is used to refer to all legal information professionals.
14. Victor Li, “60 Sites” Session Takes In the Crowd’s Favorites, A.B.A. J. DAILY NEWS (June 1, 2014, 3:00 AM CDT), http://www.abajournal.com/magazine/article/60_sites_session_takes_in_the_crowds_favorites/.
20. Allison Brecher, 8 Tips for Corporate and Outside Counsel to Protect Client Data, LAW TECH. NEWS, Apr. 4, 2014 (available on LexisNexis).
22. Richard J. Bortnick, Perspectives: Lawyers Need to Put Cyber Security Policies in Place, BUS. INS.
working to illegally access or block access to data. For example, the Public Access to Court Electronic Records (PACER) system was reportedly the target of a denial-of-service attack in January 2014. In 2013, the Washington state court system was attacked. The attack reportedly resulted in the potential breach of 160,000 social security numbers. At the 2014 E-courts Conference, organized by the National Center for State Courts, Bryant Baehr, Chief Information Officer of the Oregon Judicial Department, acknowledged that courts are targets of cyberattacks; he suggested that, in response, they use encryption and two-factor authentication for access to critical systems.

University systems supporting professional schools, including law schools, have increasingly become cybertargets. According to a July 2013 New York Times piece, U.S. universities are increasingly under attack, with “millions of hacking attempts weekly.” In February 2014, the University of Maryland reported that it had been attacked and hackers accessed Social Security numbers from more than 300,000 individuals. In 2010, Ohio State University experienced a similar data breach. Further, as students have continued to increase their use of mobile devices to conduct educational activities via university networks, security becomes increasingly important. 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 health 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 the 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.

29. While law school clinical work would not be subject to trade regulation, the recent aggressiveness of the Federal Trade Commission (FTC) in pursuing claims of unfair trade practice claims against companies that fail to take adequate data security measures is an example of increasing regulatory enforcement based on security concerns. FTC action on data security matters has been a topic of discussion in recent legal news sources. Todd Taylor & Karin McGinnis, Trade Commission Takes
In addition, academic law librarians who teach legal technology classes now recognize the need to familiarize themselves and their students with data and cybersecurity concerns. In teaching such classes, librarians typically integrate data security and ethics discussions with the coverage of other technology-related topics. For example, librarians might discuss that while security experts view encryption as a “basic safeguard” whose use should be a “no-brainer” for organizations, full-drive and e-mail encryption use in firms remains “low.” Thus, “[a]ttorneys who do not use encryption on laptops, smartphones, and portable devices should consider the question: Is failure to employ what some consider a no-brainer solution taking competent and reasonable measures” to protect client information as required by the ethics rules? Notwithstanding the involvement in legal technology classes, there is little evidence that academic law librarians are lending their talents to and leading strategic institutional efforts in the area of data security and cybersecurity.

Despite assertions today that security is “everyone’s business,” law librarians often still marginalize security concerns, believing that security is the responsibility of information technology (IT) departments. 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 access is reflected in the preamble of the American Association of Law Libraries’ (AALL) Ethical Principles:

---

30. A presentation at the 2014 Mid-America Association of Law Libraries Annual Meeting focused on the legal technology course offered at Valparaiso Law School. One presentation slide entitled “Learning About and Selecting Topics” indicates that the law librarians had to familiarize themselves with some topics. Further, the instructors list the first two topics for the course as “data security” and “cloud computing resources and ethics.” Emily Janoski-Haehlen & Jesse Bowman, Teaching Technology to the “Techie” Generation, MID-AMERICA ASSN OF L. LIB. ANN. MEETING (2014), http://maall.wildapricot.org/Resources/Documents/TEACHING%20TECHIE%20GENERATION.pdf.


32. Id. Andrew Perlman takes a similar view that understanding the importance of encryption is required by the competence requirement of the standards of conduct:

The particular safeguards lawyers need to use will necessarily change with time. For now, and at a minimum, competent lawyers need to understand the importance of strong passwords (lengthy passwords that contain a mix of letters, numbers, and special characters; the word ‘password,’ for example, is a lousy password), encryption (both for information stored in the ‘cloud’ and on the ‘ground,’ such as on flash drives and laptops), and multifactor authentication (ensuring that data can be accessed only if the lawyer has the correct password as well as another form of identification, such as a code sent by text message to the lawyer’s mobile phone).


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.35

However, the commitment to open access should not overshadow all other principles, and the AALL Ethical Principles also note that AALL members “uphold a duty to our clientele to develop service policies that respect confidentiality and privacy.”36 Service polices certainly must address access to electronic and digital resources and data and take into consideration the reasonable steps needed to minimize the risk associated with access to protect the confidentiality of users.

¶10 Further, as law librarians increasingly manage both library and IT functions or serve as chief information officers (CIOs), their marginalization or delegation of security concerns can no longer be justified. This is particularly true in cases where there are no or few IT or technical support staff.37 Even when law librarians are not responsible for IT functions, they must recognize that security “is an enterprise issue, and that means that attorneys, firm management and support personnel [including law librarians] need to be involved.”38 There are some actions that law librarians might consider to assist in reducing security risk. 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. This requires a conversation about the library’s mission and audience.39 To facilitate these conversations, law librarians have to become more familiar with the security environment and the possible risks associated with the products and services provided.

¶11 Law librarians who are not familiar with the details of today’s security environment should concentrate first on becoming more aware of security risks. Reviewing texts addressing these security concerns, such as The ABA Cybersecurity Handbook40 and Locked Down: Information Security for Lawyers,41 is a first step. With increasing frequency, the ABA Continuing Legal Education (CLE) offerings include cybersecurity topics.42 Participating in such CLEs, both as continuing learners and presenters, is a means of gaining additional knowledge and raising the profile of law librarians in dealing with data security and cybersecurity.

36. Id.
37. Thirty-seven percent of respondents to the 2013 ABA Legal Technology Survey reported that their firms had “no technical support staff at all locations combined.” AM. BAR ASS’N, 2013 LEGAL TECHNOLOGY SURVEY REPORT, at I-vii (2013).
¶12 Some security professionals indicate that education is perhaps the most important step, in part because individual firm employees are primary sources of information leakage. Yet it is interesting to note that the ABA TechReport 2013’s Security Snapshot: Threats and Opportunities reveals that thirteen percent of the respondents to the 2013 ABA Legal Technology Survey reported that “they simply didn’t know if their firm had technology policies in place”; thirty percent of the same respondents revealed that their employers offered no technology training. And the International Legal Technology Association Survey of almost 500 firms reflected that sixty-seven percent of the responding firms did not have a security awareness training program for users.

¶13 With so many attorneys unsure about technology policies or untrained in using technology safely, one growing trend is causing special concern within the legal community. Bring Your Own Device (BYOD) programs allow users to use their own devices to conduct business. Although seventy percent of respondents in a 2012 survey of law firm CIOs agreed that “BYOD programs produce ‘more cheerful users’” within the firm, failure to adequately assess and address the security risks associated with BYOD programs is a serious problem. Recognition of this concern, in 2013, led one commentator to question whether Bank of America’s cybersecurity audits of its law firms could be “the beginning of the end of the BYOD era?” However, BYOD does not appear to be going away. Daniel Burris, a technology forecaster, predicted in 2012 that BYOD “is not only here to stay but that it will continue to accelerate.” In fact, the percentage of respondents to the ABA Legal Technology Survey reporting they used “personally owned smartphones” to perform law-related work increased from sixty-five in 2012 to sixty-seven percent in 2013. It seems that technology users are not only using their own

43. See Ed Finkel, Inside-Out Threat: Law Firms’ Own Employees Are Among the Major Cyber-threats to Be Protected Against, A.B.A. J., July 2014, at 28.
45. AM. BAR’ Ass’N, supra note 37, at I-xiii.
50. AM. BAR’ Ass’n, supra note 37, at VI-xxi. It should be noted that this reflects an overall percentage and percentages varied slightly depending on the size of the firm, with solo practitioners reporting the highest percentage of those using personally owned smartphones.
devices more but are also using software specific to these devices and “consumer-oriented cloud services,” thus broadening the trend into Bring Your Own Technology (BYOT). In such an atmosphere, educating library patrons about the risk of accessing resources on these devices is essential.

¶14 Further, since mobile devices and technologies are here to stay, law librarians, IT staff, and organizational administrators must continue to develop creative means to protect data. Fortunately, some guidance is available. The International Legal Technology Association (ILTA), for example, announced in May 2012 that it was launching the LegalSec Initiative, designed in part to develop standards and templates for security programs. Yet information about progress made as a result of the LegalSec Initiative appears to have had limited distribution.

¶15 The U.S. Commerce Department’s National Institute of Standards and Technology (NIST), at President Obama’s direction, has developed “a ‘cybersecurity framework’ to help regulators and industry participants identify and mitigate cybersecurity risks that could potentially affect national and economic security.” The framework is intended for adaptation to a variety of organizational structures, and organizations are to be able to use the framework 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. However, the framework has received some amount of criticism.

¶16 In June 2013, NIST 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

1. Have a mobile device security policy that defines the types of devices permitted, the resources that may be accessed and how provisioning is handled.
2. Develop system threat models for mobile devices and the resources that are accessed through mobile devices.
3. 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.

51. Id.
52. Using storytelling about incidents of breach may serve as a motivational component of the educational experience. Julia Montgomery, Once Upon a Data Breach: How Story Telling Can Make You the Hero of Your Firm's Security Awareness Program, Peer to Peer, Fall 2014, at 56, 57, available at http://epubs.iltanet.org/i/411912. Law librarians can conduct research and use the references outlined in this work to add the aspect of storytelling to security education.
54. However, several references to the LegalSec Initiative and some information about the standard on which LegalSec is “focused” is available in the Security-themed Fall 2014 issue of Peer to Peer. Herman et al., supra note 33, at 88.
57. Id. at 18.
4. Should implement and test a pilot of their mobile device solution before putting
   the solution into production.
5. Should fully secure each organization-issued mobile device before allowing a user
   to access it.
6. Should regularly maintain mobile device security.\(^60\)

\(^17\) Certainly law librarians could and should assist in developing models for
reducing potential threats regarding how legal resources are accessed, as recom-
manded by the NIST guidelines summarized above. Law librarians might advocate
for a “spirit of compromise” that balances convenience with reduced risk.\(^61\) For
example, law librarians could advocate for an information structure that encour-
gages e-book users to download materials to their mobile devices using secure net-
works rather than insecure wireless networks. Such programs would likely also be
appreciated by users who have capped data plans on their wireless devices.

\(^18\) Law librarians should also advocate for and select security solutions such as
mobile device management (MDM) products and services. The *ABA Cybersecurity
Handbook* advises law organizations that permit personal devices on their networks
to use MDM as a “centralized way to manage mobile devices remotely, including
significantly the ability to lock or erase a lost device remotely and check its geo-
graphic location.”\(^62\) There are a number of leaders in MDM products and services,
including Airwatch, Good Technology, and Mobile Iron,\(^63\) but security experts sug-
gest that MDM is the “bare minimum” for organizations allowing BYOD. Security
options for such organizations include “MDM, mobile application management,
container-based apps, mobile virtualization, mobile backend as a service, or MBaaS,
network access control, and software defined networking.”\(^64\) However, use of a par-
ticular security technology does not ensure success. As one writer adeptly
summarizes,

\[\text{[t]he issue of managing all mobile devices, both user-owned and firm-supplied, is clearly one that extends beyond tracking inventory and basic security. It requires a comprehensive plan that starts at the top with management buy-in to firm wide policies relating to usage, sanctioned apps, access to corporate data, and auditable procedures to protect sensitive client data in the event of stolen devices. Regardless of the technology used, these strategies will be less than successful without a formal process to educate users regarding appropriate use of mobile devices and their responsibility to act in the best interest of the firm and its clients.}\] \(^65\)

\(^19\) This focus on education applies to all law-related organizations, and librar-
ians may assist by evaluating security products and services and participating in the
educational process. Hopefully law librarian involvement in the educational process

---

60. *New Federal Guidance for BYOD Security Released*, INFOLAWGROUP LLP (June 26, 2013),
http://www.infolawgroup.com/2013/06/articles/mobile/nist_sp800-124r1/.
62. RHODES & POLLEY, supra note 40, at 19.
63. NELSON ET AL., supra note 41, at 79.
64. Fred Donovan, *MDM Is “Bare Minimum” for Enterprises Dealing with BYOD, Says Analyst*,
dealing-byod-says-analyst/2012-12-02.
will result in improved security practices so that one-third of our organizations do not “allow personal mobile devices (e.g., tablets, laptops, smartphones) to access the firm’s [or organization’s] network” without the imposition of security restrictions.\textsuperscript{66}

¶20 Law librarians are increasingly involved in vetting apps used by those in the legal community.\textsuperscript{67} One of the criticisms of some MDM security services is that they foreclose the use of particular apps. A 2011 ALM Legal Intelligence Report notes that while only seven percent of survey respondents indicated that their firm had implemented a MDM platform, fifty-three percent of the users in such firms indicated that the system had “limited, in some way, the usefulness of the device”; specific examples identified the limitation of apps as a concern.\textsuperscript{68} Law librarians could make themselves even more valuable by addressing security concerns in the apps they assist in developing\textsuperscript{69} and collaborating with app developers, who may be lawyers and law students working to address access to justice concerns,\textsuperscript{70} to overcome the security characteristics that make some apps unacceptable for use by their legal organizations.

¶21 While evaluation of MDM products and services and implementation of other security measures may seem to require higher levels of technological knowledge, there are less complex measures that may be helpful. Password development and storage are areas that are relatively simple. At a 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 do not have to be technology experts but, at “the very least, . . . should know how to develop strong passwords that will be difficult to compromise.”\textsuperscript{71} 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

\begin{itemize}
  \item Responses to the 2013 ABA Legal Technology Survey indicated that one-third of the respondent firms allowed mobile device access to their networks without the discussed security restrictions. \textit{Am Bar A’ssn, supra} note 37, at I-48. In 2014, slightly more than thirty percent of the respondents to the Legal Technology Survey indicated that the firm allowed personal mobile devices to access the firm’s network without restrictions. \textit{Am Bar A’ssn, 2014 Legal Technology Survey Report}, at I-45.
  \item ALM Legal Intelligence, \textit{Productivity in the Legal Profession: The Impact of Mobile Technology} (2011).
  \item The Hackathon Workshop at the AALL 2014 Annual Meeting provided an opportunity for law librarians and programmers to work together to develop useful apps. \textit{W-1: AALL Hackathon: Building the Information Future, Am. Ass’n of Law Librs.,} \url{http://www.aallnet.org/AMhackathon} (last visited Feb. 16, 2015).
  \item James Podgers, \textit{You Don’t Need Perfect Tech Knowhow for Ethics’ Sake—But a Reasonable Grasp Is Essential}, A.B.A. J. Daily News (Aug. 9, 2014, 6:00 PM CDT), \url{https://web.archive.org/web/20140814014255/http://www.abajournal.com/news/article/you_dont_need_perfect_tech_knowhow_for_ethics_sake--but_a_reasonable_grasp} (retrieved from the Internet Archive). Perlman has noted that attorneys also need to be aware of the importance of encryption and multifactor authentication. Perlman, \textit{supra} note 32.
\end{itemize}
birthdate or password123 are not strong . . . ”72 While some may argue that strong passwords alone are not as secure as a biometric measure or security tokens that provide two-factor authentication,73 it appears that for now strong passwords remain most commonly used, considering they are not as complex to implement. It is surprising, then, that according to ILTA’s 2013 Technology Survey, twenty-one percent of the respondents did not force the use of a password to unlock mobile devices.74 Law librarians can assist others by recommending tools that generate random passwords, test the strength of existing passwords75 (e.g., Telepathwords76), or manage passwords77 (e.g., LastPass78).

¶22 In summary, security is a growing concern in all legal organizations. With new technological advancements come new opportunities, threats, and security solutions. No longer can law librarians delegate all security responsibilities to the IT Department staff. Law librarians need to be aware of the security environment and need to participate in organizational security policy development, security product and service selection, and security educational efforts. With our skills in knowledge management and document preservation, we may also contribute greatly to “cyberattack response teams.”79 If we creatively find opportunities to assist with issues of organization cybersecurity, we will add immeasurable value to our organizations.

72. Podgers, supra note 71. Failure to change default passwords (like 1234) was noted as the security weakness allowing access to home video systems and the posting of such video recordings from 100 countries to a Russian web site. Amelia Smith, Russian Website Streams Footage from Thousands of Hacked Webcams, NEWSWEEK (Nov. 20, 2014, 10:00 AM), http://www.newsweek.com/russian-website-streams-footage-thousands-hacked-webcams-285721.

73. Victor Li, Be Vigilant About Protecting Sensitive Client Data with These Tools, A.B.A. J. L. NEWSNow (June 1, 2014, 3:10 am CDT), http://www.abajournal.com/magazine/article/be_vigilant_about_protecting_sensitive_client_data_with_these_tools.

74. 2013 Technology Survey, supra note 46, at [132]. In 2014, seventeen percent of the responding firms continued to report their firms did not force the use of a password to unlock mobile devices. 2014 Technology Survey, supra note 46, at [212].

75. Li, supra note 14.


79. Stuart D. Levi & Jessica Cohen, A Weak Response Can Also Bring Lawsuits: States Are Cracking Down on Companies that Lag in Reporting Data Security Breaches, NAT’L J., Nov. 24, 2014, at 12, 13. “Cyberattack response teams” are discussed more often in the context of companies such as large retailers. However, as law firms and other organizations in the legal community increasingly find themselves targets of cyberattacks, the legal community, like other industries, must start to think of establishing plans and internal bodies to respond to cybersecurity incidents. Doug Brush, Ask the Vendor: What’s One Tip You’d Offer on How to Improve Security in an Organization? Develop an Incident Response Plan, PEER TO PEER, Fall 2014, at 22, available at http://epubs.iltanet.org/l/411912.