Cybersecurity & Law Firms: A Business Risk

Volume 39 Number 4

By Jody R. Westby

About the Author

Jody R. Westby is CEO of Global Cyber Risk LLC and the coauthor of four books on privacy, cybersecurity programs, cybercrime and ESPs. She chairs the Privacy and Computer Crime Committee in the ABA Section of Science and Technology Law and is leading the critical infrastructure working group of the ABA Cybersecurity Legal Task Force.

Law firms have never been very good with technology, and now they are struggling, as breaches in firms have made headlines and clients increasingly are asking questions about their security programs. The FBI has issued warnings to firms and held a meeting in early 2012 with about 200 firms in New York to discuss the risk of breaches and theft of client data. Around the same time, Alan Paller, director of research for the SANS Institute, a cyber training organization, revealed an amazing conversation that he had with partners from a New York firm who had been told—and shown—by the FBI that *all* their client files had been stolen. These warnings and many other instances of law firm data breaches have come squarely in the crosshairs of the ABA. Laurel Bellows, president of the ABA, has raised awareness within the legal community about cyber risks by launching a special Cybersecurity Legal Task Force to analyze a wide range of issues, including risks to law firms.

THE NEED FOR AN ENTERPRISE SECURITY PROGRAM

Many firms are now asking, “What do we do to keep our systems and data safe? How can we keep this from happening to us?” There is a simple answer to this question: Hire a chief information security officer, give him or her a budget to hire the staff needed to build and maintain an enterprise security program (ESP), and exercise appropriate governance over the firm’s digital assets.

Law firms are basically the same as any other company when it comes to countering cyber attacks and protecting their confidential

Cybersecurity Best Practices and Standards

A number of organizations and entities have wrestled with the issue of what steps are required to construct and implement a viable ESP, thus keeping client information protected. The cybersecurity best practices and standards that have been developed by these organizations and entities are listed below.

- The International Organization of Standardization, the 27000 series
- Information Technology Infrastructure Library (ITIL)
- International Society of Automation (ISA)
- Information Systems Audit and Control Association (ISACA), the Control Objectives for Information and Related Technologies (COBIT)
- Payment Card Industry Security Standards Council (PCISSC)
- National Institute of Standards and Technology (NIST) Special Publication 800 (SP-800) series and Federal Information Processing Standards (FIPS)
- Information Security Forum (ISF) Standard of Good Practice for Information Security
- Carnegie Mellon University’s Software Engineering Institute, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP)
- U.S. Nuclear Regulatory Commission

Mission Statement of the Cybersecurity

and proprietary data. The only difference is that law firms have ethical rules that require confidentiality of attorney-client and work product data. That does not make them special, however, because accounting firms, engineers and medical providers also have privileged data. All companies—irrespective of whether they are engaged in expensive research and development, processing financial transactions, providing electricity or practicing law—must have a security program that comports with internationally accepted best practices and standards. (See "Cybersecurity Best Practices and Standards" box.)

This is usually where attorneys' eyes glaze over and they want to call in their "IT guy" and go back to work. Not so fast. Security is an enterprise issue, and that means that attorneys, firm management and support personnel need to be involved.

Some basic activities must be undertaken to establish a security program, no matter which best practice a firm decides to follow. (Note that they are all harmonized and can be adjusted for small firms.) Technical staff will manage most of these activities, but firm partners and staff need to provide critical input. Firm management must define security roles and responsibilities, develop top-level policies and exercise oversight. This means reviewing findings from critical activities; receiving regular reports on intrusions, system usage and compliance with policies and procedures; and reviewing the security plans and budget.

The basics of an ESP, including the roles and responsibilities of all personnel, are provided in a security program guide developed by Carnegie Mellon University's Software Engineering Institute. A simplified listing of the activities required to establish and maintain an ESP that has been tailored toward law firms is provided below:

- Establish a cross-organizational team comprised of practice chairs, procurement (they buy copiers, faxes and printers, which have servers inside), finance, human relations, communications, office management, IT and security personnel. Meet quarterly.
- Set the "tone from the top" and issue high-level policies regarding the privacy and security of firm data. This includes the use of encryption, remote access, mobile devices, thumb drives, laptops, Wi-Fi "hotspots," clouds, Web email accounts and social networking sites.
- Inventory the firm's software systems and data, and assign ownership and categorizations of risk. Client data may need to be compartmentalized; not all clients are equal. Extremely sensitive matters have the highest risk and could cause the greatest magnitude of harm if breached. Firms may want to keep this data on a separate server with stronger security protections and stronger access controls.
- Identify points of contact with law enforcement, Internet service providers and the communications companies that service the firm, and cyber forensic experts. If the firm has multiple offices, this should be done for each, with particular attention to foreign offices.
- Conduct third-party vulnerability scans, penetration tests and malware scans. Antivirus software is essential, but it detects only a small percentage of new malware. Specialized services that detect sophisticated attacks may be required.
- Perform software code reviews on Web applications and custom code to detect vulnerabilities.

Legal Task Force

The ABA Cybersecurity Legal Task Force will identify and compile resources within the ABA that pertain to cybersecurity, and will focus and coordinate the ABA's legal and policy analyses and assessments of proposals relating to cybersecurity.

Composed of ABA members with expertise in cybersecurity as well as government, technical and private sector representation, the Task Force will

1. facilitate collaboration and information exchange among constituent ABA entities and with relevant public agencies and private organizations;
2. serve as a clearinghouse among ABA entities regarding cybersecurity activities, policy proposals, advocacy, publications and resources;
3. study and analyze executive and legislative branch cybersecurity proposals;
4. identify cyber-related issues for appropriate action by the ABA, including filling gaps in policy, encouraging ABA entities to develop new policy as appropriate, and sharing best practices with members and their law firms; and
5. advise and assist the ABA Governmental Affairs Office on cybersecurity advocacy and responses to government actions.

The Cybersecurity Legal Task Force Update

By Sharon D. Nelson

The ABA Cybersecurity Legal Task Force, chaired by Judy Miller and Harvey Rishikof, is hard at work on the *Cyber and Data Security Handbook*. The *Cyber Incident Response Handbook*, which

- Enough data is now gathered to develop a security strategic plan (a two- to five-year plan) and security program plan (the firm's 12-month plan for security activities, which will include remediation activities identified in scans and penetration testing).
- Deploy needed security technologies for encryption, intrusion prevention and detection, monitoring, security event management, etc.
- Identify and document security controls.
- Establish security configuration settings, access controls and logging.
- Develop security policies and procedures to support the security plan and technologies.
- Conduct training (general awareness, governance, operational and technical).
- Develop incident response, business continuity or disaster recovery plans and communications plans. Test them.
- Develop contractual security requirements for outsourcing vendors, cloud providers or other entities that connect to the firm's network, including notification in the event of a breach.
- Conduct regular reviews of the security program and update as necessary.

Some attorneys may fall into the trap of believing that the less they know about security threats to their system, the better. Security will never be bulletproof, but security fools are not treated kindly. Law firms, like any other business, are subject to breach notification laws, and many of them have pre-breach security program requirements. A firm will be in a far superior position with its clients, its state bar and any regulators that may become involved if it can show that (1) its security program is aligned with best practices, (2) its management is engaged, (3) it is complying with its policies and procedures, and (4) tools are deployed to detect malware and criminal behavior.

RESPONDING TO AN INCIDENT

Having a well-rehearsed incident response plan is critical. It must specify who will be notified, within what time frame, what documentation must be kept, who is designated to speak about the incident and who has authority to make certain decisions about the investigation. Serious incidents require specialized assistance from cyber forensic experts and careful documentation to preserve evidence. This is no time to learn on the fly.

While law firms need ESPs just like all businesses, special considerations arise at the time of an incident. With any breach, an almost instinctive reaction is to cover up the event and keep it secret. Paller's previously mentioned conversation with the New York attorneys revealed, in stark terms, their intention to tell no one about the breach: "Are you crazy? Can you think of a better way to destroy their trust in us than letting them know we had lost every document they gave us under [attorney-client] privilege?"

Even if the event did not trigger a breach law, a law firm's decision to cover up an incident can be a dangerous strategy. Some of the attacks against firms are suspected of having been sponsored by nation-states, and pushing these incidents under the rug may result in even further infestation of malware or exfiltration of data. Even large communication providers do not have the capabilities to

originated with the Task Force, is expected to be completed and published by the ABA Section of Science and Technology Law in spring 2014. They plan to keep the books to a reasonable length, to include graphics and checklists, and, of course, to write them in plain English as much as possible.

The Task Force is looking at how China and other nations are breaking into law firms. What security measures are reasonable, and at what point do you tell clients about a breach? Does it make sense to draft a resolution of some sort? Have ethical obligations changed with technology and the nature of the threat? Are there different obligations for small and large firms and, if so, how should we determine them? One suggested solution is to let the client host the data in the matter you are working on for them. Then it would be up to the client to make sure that privilege is not broken by unauthorized people having access.

The government has divided critical infrastructure into 16 sectors—and legal isn't one of them. Should there be a legal information-sharing environment technology system? There are a lot

ward off a nation-state without government assistance; to think that a law firm could is laughable. If investigated, some might consider this negligent behavior.

ETHICAL CONSIDERATIONS

Firms must also consider that ethics rules already have provisions addressing metadata and email, so if either of these were disclosed, an ethics issue is already in play. Whether a firm is ethically obligated to report a security breach of attorney-client documents to its clients is a question that many security professionals have bandied about.

New commentary to Rule 1.1 of the *Model Rules of Professional Conduct* requires attorneys to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." So the days of attorneys being technology troglodytes are over. Model Rule 1.6(c), on the confidentiality of client communications, acknowledges that disclosures can happen by providing: (c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Commentary on the Rule notes that [18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure.

Thus, Rules 1.1 and 1.6 may allow a law firm to avoid an ethics violation stemming from a breach if it has acted in a competent manner (e.g., having a strong security program) to protect its client data from disclosure.

Rule 1.6(c), however, does not address whether attorneys have to tell their clients about such an event. Law professor Benjamin Cooper's *Baylor Law Review* piece, "The Lawyer's Duty to Inform His Client of His Own Malpractice," raises some very interesting points about self-reporting of negligence. In addition to discussing Rule 1.4 (communications with the client) and the fiduciary law governing the lawyer-client relationship, he explains that the *Restatement (Third) of the Law Governing Lawyers* states: "If the lawyer's conduct of the matter gives the client a substantial malpractice claim against the lawyer, the lawyer must disclose that to the client."

When I recently spoke with Professor Cooper, he observed that "firms have a duty under Rules 1.1 and 1.6 to effectively protect their clients' information. If a firm is negligent in carrying out that duty because it has been lax with its security, and that resulted in client files being disclosed, it is potentially a problem." Even if a firm has a very good security system, he observes that "the attorney absolutely has a duty to inform clients under 1.4 that their confidential information has been compromised."

of questions—more questions than answers at the moment. And the Task Force has a short life span. Its work, which began in August 2012, is slated to be completed by this August.

More information about the Cybersecurity Legal Task Force may be found at americanbar.org.

Accordingly, a strong security program may help shield a firm from an ethics violation caused by not appropriately protecting client data, and it may help them beat a negligence charge, but it has no impact on the Rule's requirement to inform clients of security incidents. A good security program does, however, reduce the likelihood that such a painful conversation will have to take place. All together, it is clear that an up-to-date security program is the best defense that a law firm can have. Whether large or small, taking measures to establish a strong security posture is not only the right thing to do, it's the ethical thing to do. It may help save the firm cases, clients and its reputation.

"We live in a world where our national security is threatened by cyberterrorists, and where private enterprise is forced to respond to cybertheft of intellectual property on a daily basis. The ABA Cybersecurity Legal Task Force is examining risks posed by criminals, terrorists and nations that seek to steal personal and financial information, disrupt critical infrastructure and wage cyberwar. When our national security and economy are threatened, lawyers will not stand on the sidelines."
–Laurel Bellows
2012-2013 President of the American Bar Association

4 Steps to Getting Serious About Law Firm Cybersecurity

BY JOSEPH M. BURTON ON SEPTEMBER 15, 2014 ·

The need for better cybersecurity, along with the responsibility to safeguard client and firm information from the risk of loss from cyberattack, has been the focus of considerable discussion by law firms for the past four years. While some law firms have recently awakened to this key issue, significant further work needs to be undertaken. Let's look at the progress (or lack thereof) of law firm security over this four-year period — and four ways firms could improve both the speed and effectiveness of their cybersecurity going forward.

The Treasure Trove

When asked why he robbed banks, Willie Sutton reportedly replied: "Because that's where the money is." From the perspective of today's cyber-criminal, law firms may not have much cash lying around, but they have a treasure trove of valuable information—the universal currency of the 21st century.

Almost all law firms of any size or legal specialization have in their custody and control sensitive client and firm-business information. Right this minute, law firms have all or some combination of the following:

- case and/or litigation strategy information, including settlement parameters and argument weak points;
- confidential client business information (this information may be either retrospective information about the circumstances of the matter at hand, or *prospective* information about future plans and initiatives – or both);
- attorney-client privileged communications and other legally privileged information (such as attorney work product);
- client intellectual property, such as patent, copyright and trade secret information;
- a range of personally identifiable information (PII) of all kinds for employees, clients and third parties, such as personal health information and various account and account-access information that include customers' name and address information; and
- payment card information, including card numbers and PIN numbers.

In short, firm confidential information includes much information for which the firm has a legal, ethical or business requirement to protect from disclosure or compromise.

Ethical Responsibilities

The ethical standards to ensure that attorneys and firms maintain the confidentiality of all information relating to the representation of a client are well-known. ABA Model Rule 1.6(c) requires that *"[a]lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."* Most states have similar ethical provisions. In addition to the ethical rules, bar-governing authorities have issued a number of opinions interpreting their respective rules regarding confidentiality in the context of digital information.

In a 2011 opinion, the ABA considered Rule 1.6 in the context of the duty to protect client email communications between a lawyer and the client. The ABA opinion noted that:

"a lawyer must act competently to protect the confidentiality of clients' information. This duty, which is implicit in the obligation of Rule 1.1 to 'provide competent representation to a client,' is recognized in two Comments to Rule 1.6. Comment [16] observes that a lawyer must 'act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.'"

In 2010, the State Bar of California considered whether the duty of confidentiality was violated by the use of technology to transmit and store confidential information when the technology was susceptible to unauthorized access by others. Specifically, the California Bar reviewed a matter in which an attorney used his personal laptop to work on a client's information from home; access a public Wi-Fi network to conduct legal research for the client's matter; and communicate via email with the client while away from his office. The California Bar analyzed this issue by reference to the attorney's duty of competence. The opinion concluded that: *"An attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure. Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps." (Emphasis added.)*

Legal Responsibilities

In addition to these ethical requirements, some of the information stored and used by law firms on behalf of their clients, as well as in management of the firm itself, is subject to statutory, regulatory and contractual requirements regarding the use and protection of the information. Well-known examples of this type of data protection are the HIPAA Data Security Regulations and the HIPAA Privacy Regulations (see here and here).The January 2013 amendments to the regulations expanded the definition of "business associate" in a manner that encompasses law firms performing legal services for a "covered entity," such as a doctor, hospital or other healthcare entity. Law firms that possess and use protected health information (PHI) are required to handle that information in conformance with the HIPAA data security and privacy regulations.

The data security regulation requires that covered entities and business associates have a data security plan setting out reasonable steps to be taken to ensure the security of PHI. The regulation borrows heavily from the long-standing guidelines of the Gramm-Leach-Bliley–inspired "Safeguards" rule. Law firms with such information must "protect against *"reasonably anticipated uses or disclosures* of the protected information," but are given the leeway to do so in ways that take into account the probability and criticality of potential risks to the protected health information, the implicit and capabilities of the business and the costs of security measures. Finally, a business associate has to periodically review and modify implemented security measures.

A number of states have enacted statutes that protect the personally identifiable information (PII) of their citizens and specifically require individuals and any business that does business in the state to encrypt, under certain circumstances, PII used by the business. In 2008 and 2009, Nevada and Massachusetts became the first states to pass such provisions. The Massachusetts data security regulation requires encryption of PII that is transmitted over the Internet. Law firms having offices in or otherwise doing business in Massachusetts must comply with this regulation or face potential civil and/or criminal penalties.

Similarly, law firms with offices in countries that are members of the European Union (EU), or who handle and store protected personal information pertaining to citizens of the EU that they have received from or on behalf of their clients, are under similar requirements to take measures to ensure the security of that information. Currently, this is an indirect result of the EU's broad data privacy regulations (see here and here). However, the EU is now considering new and very specific data security regulations that would more specifically and comprehensively cover the protection of this information.

Lawyers are under both ethical and legal requirements to safeguard a large range of the information that flows into and out of their firms. However, too many firms have been either unaware of the risks of compromising this sensitive information or have not taken those risks seriously.

Asleep at the Switch

In 2009, the FBI issued an "alert" advising law firms that they were being specifically targeted by organized cybercriminals through the use of email phishing campaigns. This was only the beginning.

The cybercriminals discussed in the FBI's alert and those behind subsequent law firm breaches are just one of the groups within a vast network of sophisticated, highly organized and well-funded criminal organizations. These groups are often, but not primarily or exclusively, foreign-based. They are sometimes state-funded, and like Willie Sutton, their motivations for breaching law firm security and stealing confidential information are primarily economic.

Given the sophistication and economic power of these organizations, one might think their methods would be equally sophisticated. They are. The techniques used to steal from law firms and other high-value targets are stealthy, persistent and challenging to detect. Because of these characteristics, they are sometimes referred to as advanced persistent threats (APT). In addition to the methods used to effectuate these attacks, APT attacks are known for their use of sophisticated targeting techniques that are aimed at high-level individuals within the law firm or corporation being attacked, and which often feature meticulously crafted email messages designed to fool even careful readers.

In 2010, several news stories revealed law firm data breaches and chided firms on their absence of security and attention to what appeared to be a growing problem. A good example is a March 2010 article in the *National Law Journal* titled "Firms Slow to Awaken to Cybersecurity Threat,"which included comments by Mandiant (a digital forensics firm that would later become famous for its data breach work for the *New York Times*, the State of North Carolina and in other high-profile cybersecurity incidents) that it had been involved in the investigation of over 50 law firm data breaches.

The same year, a Los Angeles-based law firm, Gipson, Hoffman & Pancione, publicly revealed that it had been the subject of a sophisticated phishing attack, which the firm and its forensic experts believed originated from China. A week before the attack, Gipson had filed a $2.2 billion copyright infringement suit against the People's Republic of China on behalf of its client. At the time, this attack was widely covered by the press, including the *Wall Street Journal* and others. The *Journal* quoted a member of the firm as stating: "They were e-mails targeted at individuals in our law firm that were made to appear as if they were coming from other individuals at our law firm," he said. "They attempted to get the target to click on a link or attachment."

Also in 2010, at least seven Toronto, Canada–based law firms were attacked in an effort to derail a $40 billion acquisition of the world's largest potash producer by an Australian mining company that was a principal competitor of the second-largest producer, a Chinese company. These attacks did not come to light until two years later.

A year later, in November 2011, the FBI invited 200 of the largest law firms to a meeting in New York to discuss the agency's concern that sophisticated cyberattacks targeting the gold mine of information that law firms hold were increasing, and its expectation was that they would continue to do so. In a January 2012 *Bloomberg* article that later discussed this meeting and law firm data breaches in general, FBI Special Agent Mary Galligan summed up the meeting this way: "Some were really well prepared; others didn't know what we were talking about."

In March 2012, Jeffrey Brandt, a well-known law firm IT professional and blogger, wrote an article titled "When Good Enough – Isn't," in which he lamented the extremely "abysmal" state of law firm security. Among other things, Brandt discussed the then-most recent (October 2011) International Legal Technology Association (ILTA) study. Some key findings from that survey were:

- 86 percent of firms **do not** use or require two-factor authentication.
- 78 percent of firms **do not** issue encrypted USB drives.
- 76 percent of firms **do not** automatically encrypt content-based email.
- 58 percent of firms **do not** encrypt laptops.
- 87 percent of firms **do not** use any laptop tracking technology.
- 61 percent of firms **do not** have intrusion detection tools.
- 64 percent of firms **do not** have intrusion prevention tools.

Law Firm Reactions

The 2011 ILTA study covered a time (between October 2010 and October 2011) before some of the public disclosures and discussion described earlier (notably the FBI meeting in New York), and when law firms may not have really been "awakened" to the issue. However, by late 2013, law firms should have taken cybersecurity and the protection of confidential information to heart—and firms should have made significant improvements to their security postures. Yet as late as November 2013, Joe Patrice, a law firm IT specialist wrote a blog post blasting the lack of attention and interest by lawyers in security issues and terming law firms the "*soft underbelly of American cybersecurity.*"

Not everyone involved in law firm security would agree that such a grim assessment. In July 2014, Judith Flournoy—a respected law firm CIO and chairwoman of ILTA's legal security working group—responded to Patrice's characterization, contending that law firms have received the message and are addressing security concerns through the use of, among other measures, client security questionnaires and audits and, perhaps most importantly, the pursuit of ISO 27001 certification.

If the concept of law firms receiving the message and actively addressing cybersecurity concerns was real and not a mirage, this would be great news, and it would perhaps signal a key turnaround in law firm thinking and action. However, ample evidence seems to indicate that such a change in attitude and action regarding cybersecurity has not yet occurred. Most firms are still not really serious about cybersecurity.

For example, the 2013 ABA Legal Technology Survey (a product of the Legal Technology Resource Center) found that no more than half of the firms responding presently had written or implemented essential cybersecurity policies, such as those covering privacy, email retention, Internet use, email use, computer use and document records management. More precisely, the survey showed that 50 percent of the firms responding had document management policies. In every other policy-related category, less than 50 percent of the firms responding had the specified policies.

Most concerning is the most recent ILTA Tech Survey. This survey reveals that while law firms arguably may have awakened recently to the substantial risks posed to their confidential information, and despite any movement toward ISO certification, what is actually being done to address these risks is far from satisfactory. Law firm reaction is perhaps best characterized as slow and tepid.

The most recent ILTA survey was released in November 2013 and encompasses the year between October 2012 and October 2013. This is a period in which firms should have been aware of the serious security risks they faced and moved to address them. The chart below compares the results of the surveys in the same seven areas discussed almost two years earlier in Jeffrey Brandt's blog.

% in 2011	Security Measure	% in 2013
86	**Do not** use or require two factor identification	76
78	**Do not** issue encrypted USB drives	72
76	**Do not** automatically encrypt content-based emails	64
58	**Do not** encrypt laptops	56
87	**Do not** employ any laptop tracking technology	90
61	Have **no** intrusion detection tools	no change
64	Have **no** intrusion prevention tools	no change

While minimal improvement was reported in some areas, the overall result is essentially the same as was described by Mr. Brandt *over two years ago*: abysmal. In the four years since this issue became publicly known on a wide scale, lawyers and law firms appear to have failed to make obvious yet essential changes that could make a difference in their security posture.

"Compliance Is Not Security"

This is a well-known saying by those who work in the information security field. It is why the mere fact that large law firms now may be making progress toward becoming ISO 27001 certified provides little comfort regarding the actual readiness and ability of firms to protect the confidential information entrusted to them.

ISO 27001 is a risk *management* standard. It describes what ends should be achieved, but not how to achieve them. Moreover, ISO 27001 is neither mandatory nor does it have a method of enforcement that can ensure that the requirements of the standard are being followed and kept up-to-date. Unfortunately, the history of the information security industry reveals that security standards are more often than not used as a checklist item (or a checklist of items) merely to attain the goal of certification, and then put aside to gather dust (if and) until the next occasion to be "certified" occurs.

Pursuit of industry standards is a useful step toward achieving organizational security objectives. However, it is not a key step, and it should not be the first step taken by law firms to meet their obligation to protect confidential information. ISO 27001 certification will likely be a trump card to play when firms are pressured to respond to security questionnaires and audit requests from their clients., It may ultimately *help* with the firm's security posture when fully and finally implemented. However, it will do little to reduce the risks firms face in the immediate and short term. It has been at least four years since the first publicly revealed attacks, and two years since the great awakening. Yet the most recent ILTA survey reflects that at present, only 2 percent (the lowest percentage for any category on the survey besides "other" at 1 percent) of firms indicate that they are ISO certified.

When law firms place emphasis on attaining ISO or any other certification, it may complicate, delay and distract firm management from well-defined steps that can and should be taken in the short term.

Toward a Better Response

By almost any objective measure, the collective actions taken by attorneys and law firms to deal with the risk of exposure of their confidential information have been anemic at best. While a minority of firms and attorneys have taken real steps and measures, most firms have done little to effectively address the risk. The actions taken seem to be focused on the wrong problems or at least on problems unrelated to the most common and most serious security risks. To have real progress and impact on the security of a firm's confidential information, two vital areas should be quickly and resolutely addressed.

Lawyer Acceptance

"I have seen the enemy and he is us." A principal cause of the lackadaisical manner in which a security risk has been handled is cultural. While firm CIOs and their staffs have awakened to the seriousness of the problem and are augmenting existing security efforts, the same cannot be said of lawyers. The bad and outdated attitudes that many attorneys have toward information security measures (and therefore necessarily, if unknowingly, their responsibility to protect confidential information) must be overcome. Many of these attitudes reflect one of the general characteristics of the legal profession: conservative by nature and slow to change habits and behavior. Lawyers, curiously enough given their profession, often dislike and are reluctant to abide by mandated rules or proscriptions. This is especially so if they do not adequately understand the particular proscriptions and the reasons behind them.

A successful information security initiative requires the cooperation of a law firm's technical (the CIO and IT staff) and non-technical (attorneys and executive staff) personnel to address this issue. This requires consensus regarding (1) the information that requires protection; (2) the nature and extent of the risks to that information; (3) the firm's risk appetite, including an understanding of the risk level to confidential information that the firm is willing and legally permitted to tolerate; and (4) the amount of resources the firm is willing and able to commit to insure that level of risk. Information risk management is not a responsibility that can or should be handled solely or primarily by the IT staff and then handed down like sacred tablets to the firm's lawyers and staff.

Failure to win the hearts and minds of the firm's attorneys (and staff) is a recipe for lethargic and/or ineffective attention to cybersecurity. To get serious about law firm cybersecurity, attorneys have to awaken to the reality of cybersecurity risk, and begin to embrace and cooperatively implement solutions.

Better Focus

Confidential law firm information faces two primary forms of risk: theft of data and leakage of data. As discussed above, awareness of and most public discussions about law firm cybersecurity risk primarily have been driven by and focused almost exclusively on high-profile theft of data. This has had the unfortunate effect of distracting and perhaps hindering firm leadership from recognizing and fully comprehending the imminent peril posed by more prevalent but equally dire risks. To get serious about cybersecurity, firms must better understand the threat landscape, and adopt measures that can reduce the risk in these two most-pressing areas of concern for law firms.

Data Theft

This form of risk has been and will remain a significant threat to law firms. As noted previously, the cybercriminals perpetuating these attacks are extremely sophisticated, and their attacks are highly targeted. Their efforts at espionage and theft are not simple-minded, poorly written "spam" email attacks, but rather, well-researched "phishing" efforts directed almost exclusively at selected individuals (very often of a high level) and law firms or other companies. Email phishing, however well done, is not the only means employed by these attackers to gain entrance to high-value systems. Last year, one of the largest and most prominent Barrister houses in Britain with very strong ties to the energy industry was the subject of a "waterhole" attack. In the simplest terms, these attacks succeed by implanting malware on legitimate (and usually highly reputable) websites likely to be visited by the target. Once the target interacts with the poisoned site, the target's computer is infected and the first stage of the attack begins.

Regardless of the means used to initially gain entry into a law firm's system, these attacks fall within in the category of APT. They are so named because having once entered a system, they are designed to remain undetected while they acquire knowledge about the operation and data layout of the system. This malware will first look for information of interest. This may be specific pre-identified information or more general categories of information of potential interest. The malware will next collect and store the identified information within the system. Finally, the collected information is exfiltrated to computers owned or controlled by the authors of the malware. In some instances, the APT malware will attempt to hide evidence of it ever having been in the system and then erase itself. In other instances, it may continue to lurk indefinitely in the system, or until it is detected and removed.

Data Leakage

Apart from the targeted and specialized theft described above, other less sophisticated, but more frequently encountered, problems may compromise confidential law firm information . The leakage of a firm's confidential information may occur through many means, including insider misuse; loss of an unsecured laptop or other mobile device; communication over public or other unsecured networks; visiting questionable websites; and downloading unapproved software onto the firm's computer network or onto a mobile device, which connects to a repository of confidential firm information. Let's briefly look at two examples.

Insider Misuse

A key form of data leakage involves law firm "insiders." "The greater hazard to private enterprises may come from insiders who have ready access to sensitive information and either misuse or mishandle it," wrote Michael McNerney and Emilian Papadopoulosin a 2012 article titled "Hacker's Delight: Law Firm Risk and Liability in the Cyber Age."

The 2014 Verizon Data Breach Investigations Report found that 19 percent of the breaches reported were the result of insider misuse. "Misuse" encompasses any intentional, non-intentional, legal or illegal activity undertaken by an insider that results in the loss or exposure of confidential data. It occurs when someone uses data in a manner counter to an organization's policies (*e.g.*, an employee sending intellectual property to his or her personal email account is an example of email misuse).

Law firm insiders include attorneys, staff and third-party partners. While Edward Snowden may be the poster child for the risks related to the disclosure of confidential information from insider abuse, such intentional criminal behavior is an aberrational, though not unheard of, concern for law firms. Recently, a former employee of Simpson Thacher & Bartlett LLP was accused of stealing client information and passing it on to accomplices as part of an insider-trading scheme. In 2011, an employee who had been fired from a Pittsburgh-based law firm used his old and unretired computer credentials to give members of the protest group "Anonymous" access to the firm's systems. Once access was obtained, the group copied various files and then erased all of the firm's files and backup files.

Communication Misuse

The communication of unsecured confidential information also poses a very high risk for data leakage. Lawyers use email each day to transmit confidential information in the normal course of performing their legal responsibilities. Only a small portion of this information is encrypted during transmission. Moreover, when encryption is used, it is often based on an ad hoc, individually determined decision and is not the result of policy requirements. A 2014 LexisNexis Report found that almost 90 percent of the respondents (a mix of attorneys from all size firms) communicated with their clients, or with privileged third parties, by email. However, only 22 percent encrypted these emails. Yet, 77 percent included a confidentiality statement in the body of the email. Another 21 percent included a confidentiality statement in the email header. Confidentiality statements provide little help for the risks of data leakage. As the report notes: "The use of the confidentiality statement conflates the duties to maintain client-attorney privilege, and the duty to protect client confidential information. … [C]onfidences, once let into an unsafe ether, are put at risk, and no 'confidentiality statement' can mitigate that."

Cloud-based file sharing services, such as Dropbox™, Box, and others, are another way confidential information leaks out of a firm. The LexisNexis survey found that 52 percent of the lawyers surveyed used such services to transmit and share client-privileged information. Typically, the cloud service is being used through the attorney's personal account, and the firm may not even be aware that files are being transmitted and stored in this fashion! To address these issues, many large firms prohibit, as a matter of policy, the use of such services for these purposes. Some firms also block access to such services from the firm's desktop computers. Unfortunately, many firms do not.

The risk posed to the firm's confidentially held information from this form of stealth data transmission and storage was illustrated earlier this year when a firm experienced the release of a client's confidential tax and real estate information. The unencrypted information had been stored on a cloud service but was, without the knowledge of the firm, made publicly available over the Internet as the apparent result of the attorney's failure to properly configure the "sharing" function of the service.

The perilous drip of confidential information out of law firms through means like those described above is because many law firms have not implemented and adhered to specific, basic, but highly effective security controls. In short, the compromise, actual or potential, of confidential information in this fashion is a self-inflicted, *but self-correctable* wound.

What Can Be Done Now

Each firm or solo practitioner's situation is somewhat different, and the particular risk-management policies, processes and security controls employed will also be different. The development, configuration and actual implementation of a law firm's final, fully-formed risk management plan is best accomplished through a risk management platform like ISO 27001 or the NIST Framework.

Several cybersecurity components are essential to a law firm's cybersecurity risk management plan. They are applicable to almost any business, but are particularly vital for law firms because of the breadth, volume and sensitivity of the confidential information handled by attorneys. The absence of, or failure to implement, one or more of these essential components significantly reduces the likelihood that a law firm would be able to successfully argue that it had employed *reasonable security* measures. These cybersecurity components can be implemented without having to wait on the development of a comprehensive cybersecurity risk-management program. After implementation, they can be later integrated into any well-designed plan. Highlighted below are four components that are listed in their relative (not absolute) order of priority.

Encryption. Encryption is the acid test of seriousness. As a matter of policy, it must be used to protect the firm's *confidential information*. It's that simple. If a firm is not encrypting its confidential information, then it is not being serious about the risk of potential compromise of that information. Confidential information should be encrypted *every time* it is transmitted into or outside of the firm. Further, consideration should be given to encrypting specified categories, or all *confidential information* at rest (stored) *within* the firm.

The manner and nature of the encryption employed may vary depending on the specific threats involved, but will nearly always provide for the encryption of laptops, cell phones and other mobile devices; and the encryption of email and file transfer related communications.

Intrusion Detection and Prevention. As discussed in this article, the likelihood of attack by sophisticated APT malware and other methods continues to pose a serious threat to the ability of law firms to maintain the security of their confidential information. This form of threat cannot be effectively addressed, let alone defeated, without using the appropriate intrusion detection and prevention tools. The early detection of this malware and the timely prevention of information loss from these forms of attack mandate appropriate use of well-trained forensic specialists; deployment of sophisticated counter espionage software; and development and maintenance of specialized threat detection and prevention hardware and software. Use of these measures *will* carry a greater cost. Nonetheless, it is essential to countering this threat. The widespread practice of having IT personnel review firewall and other system logs, and relying only on yearly (or greater) penetration testing/auditing is insufficient. For this menace, these practices most often are too little, too late.

Meaningful User Education. Law firms, much like other businesses, have neither viewed nor effectively employed user education as an essential part of good cybersecurity. Yet it is apparent that the users of law firm computing systems may constitute *the most critical* component of the security protecting the firm's confidential information. Whether analyzing the theft of information via the most sophisticated APT, or the leakage of information through transmission of unencrypted email, a common denominator defining successful attacks has been the actions that a system's user took (or failed to take) in initiating or propagating the attack.

Risky user behavior and a reluctance to embrace security protocols and procedures are often directly related to not understanding the nature of the threats to the firm's confidential information, the reasons why a particular security protocol needs to be followed or the real-life consequences of failing to do so. Firm IT "training" often does a good job at explaining the "how" of any technology or practice, but it can be far less adept at explaining the "why."

Law firms may want to begin approaching cybersecurity education as an opportunity to make each user a willing and enthusiastic protector of the firm's confidential information.

Written Policies. Law firms must have up-to-date written policies addressing key cybersecurity topics. Firms should have a breach response policy that spells out precisely, and in reasonable detail, who, what and how the firm will respond to a breach, leak or other actual or potential compromise of its confidential information. Firms also should have a computer use policy in place. This policy should describe the rights and responsibilities of the users of the firm's computers (desktop or mobile) and any other computers used to access or hold the firm's confidential information.

Conclusion

While most firms may now be more aware of the risks to their information, there is all the difference in the world between knowing that you live in a high-crime neighborhood and actually putting locks on the doors and buying an alarm system. To date, most law firms of any size have not sufficiently addressed the threats to the security of their confidential information. In addition to any damage attendant to the compromise of their information, firms also risk the potential economic and reputational fallout from being found to have violated their ethical or legal duties.

The four key measures proposed here can help firms potentially avoid this outcome by considerably diminishing the most common and recurring cybersecurity threats. They can be implemented immediately (or in fairly short order). Prompt adoption and implementation will not interfere with or delay development of more comprehensive plans and measures. Most notably, if implemented, they can *significantly* reduce the risk of compromise to a firm's confidential information. When implemented, they will represent a serious response to law firm insecurity.

About the Author

***Joseph M. Burton** (@JMBurton88) a partner in the San Francisco office of Duane Morris LLP (@DuaneMorrisLLP). He can be reached at 415-957-3014 or JMBurton@duanemorris.com.*

(Image Credit: ShutterStock)

RELATED ARTICLES

THE GLOBAL PRACTICE ISSUE | APRIL 2014

Start with the Work and the Technology will Follow

ABA TECHSHOW ISSUE | FEBRUARY 2014

The Legal Technology Proving Ground: ABA TECHSHOW 2014

THE FINANCE ISSUE | JUNE 2014

PaperLESS Office Creates Financial and Sustainability Advantages: Insights from a Law Firm COO

The New York Times

Law Firms Are Pressed on Security for Data

By
Matthew Goldstein

March 26, 2014 7:00 pm

A growing number of big corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount.

Wall Street banks are pressing outside law firms to demonstrate that their computer systems are employing top-tier technologies to detect and deter attacks from hackers bent on getting their hands on corporate secrets either for their own use or sale to others, said people briefed on the matter who spoke on the condition of anonymity. Some financial institutions are asking law firms to fill out lengthy 60-page questionnaires detailing their cybersecurity measures, while others are doing on-site inspections.

Other companies are asking law firms to stop putting files on portable thumb drives, emailing them to nonsecure iPads or working on computers linked to a shared network in countries like China and Russia where hacking is prevalent, said the people briefed on the matter. In some cases, banks and companies are threatening to withhold legal work from law firms that balk at the increased scrutiny or requesting that firms add insurance coverage for data breaches to their malpractice policies.

“It is forcing the law firms to clean up their acts,” said Daniel B. Garrie, executive managing partner with Law & Forensics, a computer security consulting firm that specializes in working with law firms. “When people say, ‘We won’t pay you money because your security stinks,’ that carries weight.”

The vulnerability of American law firms to online attacks is a particular concern to law enforcement agencies because the firms are a rich repository of corporate

secrets, business strategies and intellectual property. One concern is the potential for hackers to access information about potential corporate deals before they get announced. Law enforcement has long worried that law firms are not doing enough to guard against intrusions by hackers.

In 2011, the Federal Bureau of Investigation began organizing meetings with the managing partners of top law firms in New York and other major American cities to highlight the problem of computer security and corporate espionage, especially for law firms with offices in foreign countries like China and Russia.

Despite those meetings, F.B.I. officials and security experts say, law firms remain a weak link when it comes to online security. But the push from corporate clients may have more impact on changing law firm attitudes than anything else.

“Clients are putting more restrictions on law firms about things to do to protect themselves,” said Mary E. Galligan, an executive in the cyber-risk services division of Deloitte & Touche and the former special agent in charge of cyber and special operations for the New York office of the F.B.I. “It is being driven by victims of hackers, and they don’t want to be victims again. It’s just good business sense.”

When she was with the F.B.I., Ms. Galligan organized the meetings with managing partners of law firms to impress on them the need to better police their computer systems. The first meeting, held in New York in November 2011, was attended by top lawyers from nearly 200 firms. Over the next two years, Ms. Galligan said, she arranged half a dozen smaller meetings with law firm executives around the country. She said it had taken awhile, but she saw law firms being more proactive about computer security in large part because of the demand from clients.

Companies are prodding law firms on security at a time of overall rising concern about hacker attacks like the information breach at Target last year, when the retailer said at least 40 million credit and debit card accounts were compromised. Financial regulators are also requiring banks to make sure that vendors they rely on, like law firms, are vigilant when it comes to dealing with hackers and other online intruders.

“The public and private sectors must be riveted in lock step in addressing these threats,” Mary Jo White, the chairwoman of the Securities and Exchange

Commission, said Wednesday at a round-table discussion on the obligations of public companies to disclose online attacks. The discussion brought together more than two dozen security experts from the federal government and the financial services sector.

Still, spying by governments both at home and abroad and how that could involve a breach of client confidence is also a concern for businesses. In February, The New York Times reported that communications between lawyers at Mayer Brown, a big Chicago-based law firm, and officials with the Indonesian government were intercepted by an Australian intelligence agency that had ties to the National Security Agency, the federal agency that has been under siege for nearly a year because of its domestic spying program. The American Bar Association, with nearly 400,000 members, sent a letter to the N.S.A. to say it was incumbent on the security agency to make sure the principle of attorney-client privilege was protected.

Stuart Pattison, a senior vice president with Endurance Specialty Holdings, an underwriter of professional liability insurance coverage for law firms, said the main concern for the F.B.I. was state-sponsored hackers breaching a law firm computer system to tap into information about what American corporations were doing. He said that a few law firms had recently inquired about obtaining an added level of insurance coverage for data breaches in response to a demand from their corporate clients.

Despite the concern, it's hard to gauge just how vulnerable law firms are to attacks from hackers. There are few rules requiring firms to make public any breaches, and because the firms have little direct interaction with consumers, there is no need for them to publicly report a hacking incident the way a bank or a retailer would. In 2012, Mandiant, a security consulting firm, put out a report estimating that 80 percent of the 100 largest American law firms had some malicious computer breach in 2011. Actual reports of confidential information hacked from a law firm computer system and later winding up on some overseas server are rare, however.

Representatives for several large law firms, all of whom declined to discuss the topic publicly, said privately that the threat assessments from the F.B.I. and consulting firms were overstated. The law firm representatives said hacker attacks were usually email "phishing" schemes seeking to access personal information or account passwords, the kind of intrusions that have become commonplace and are

easily contained.

But Vincent I. Polley, a lawyer and co-author of recent book for the American Bar Association on cybersecurity, said many law firms were not even aware they had been hacked. He said a lot of law firm managers were in denial about the potential threat.

"A lot of firms have been hacked, and like most entities that are hacked, they don't know that for some period of time," said Mr. Polley. "Sometimes, it may not be discovered for a minute or months and even years."

A version of this article appears in print on 03/27/2014, on page B1 of the NewYork edition with the headline: Law Firms Are Pressed an Security for Data.

SECURITY

Law firms' own employees are among the major cyberthreats to be protected against

POSTED JUL 01, 2014 07:50 AM CDT

BY ED FINKEL

Seyfarth Shaw CIO Andrew Jurczyk says firms are vulnerable when an employee is about to leave, so the transition process should be handled systematically. Photo by Bob Stefko.

Law firms face an array of cyberthreats from foreign governments, competitors and hackers. And then there's the threat that has always existed in the offline world, but has migrated online: inside jobs—or what cybersecurity experts call extrusion.

That threat comes from firm employees who may be disgruntled or who want to make a quick buck from selling private information.

While there's no such thing as 100 percent protection against extrusion, to guard against it experts recommend tight background checks, formal written policies, perpetual vigilance, appropriate attention to technical considerations, and striking a balance between security and usability of the firm's files and data.

While inside jobs may not be common, they do happen, says Edwin Reeser, an Altadena, California, sole practitioner who writes about law management issues.

"Crowell & Moring had one guy [Douglas Arntsen, who pleaded guilty in 2012] who took a bunch of money from clients and tried to run away" and was extradited from Hong Kong, Reeser says. He also cites the case of Matthew Kluger, convicted in 2012 in an insider trading scheme that ran 17 years while Kluger worked at Cravath Swaine & Moore; Skadden, Arps, Slate, Meagher & Flom; and Wilson Sonsini Goodrich & Rosati. Reeser says Kluger "would run barefoot through the firms' system late at night because he had access and gave [information] to outsiders who traded on it. … Those could have been detected and stopped with an appropriate system."

Even smaller boutique firms need such systems and protections.

"We're going to find providers of these services … that we're going to have to hire," he says. "If you don't have $20 million to set up a system … but you don't need a system for everything you do, you're going to have to rent it." Such systems also can be accessed in concert with major corporate clients who can best afford it, Reeser adds.

To start with, firms must perform background reviews and make judgments about a potential employee's reliability during the hiring process, says Alan Charles Raul, a Washington, D.C.,

partner at Sidley Austin and author of a chapter in *The ABA Cybersecurity Handbook (http://shop.americanbar.org/eBus/Default.aspx?TabID=251&productId=213569)*. "You need intake scrutiny," he says.

Writing and disseminating formal policies helps ensure that honest personnel know to be aware of and report any suspicious activity, Raul says. Those policies should make clear that firms have the right to monitor their networks to enforce compliance and prevent wrongdoing, and that no expectation of privacy should exist in the use of the firm's network.

"The formal, written policies are not necessarily going to deter the renegade," he says. "But by sensitizing all the honest employees, you do make the environment less hospitable for dishonest employees."

Firms also need policies to appropriately restrict the use of personal handheld devices and home computers, Raul says. But policies limiting use of personal smartphones, tablets or laptops can cause some strong reactions, especially from top partners, notes Sharon Nelson, president of cybersecurity firm Sensei Enterprises Inc. in Fairfax, Virginia.

"They dictate, and IT and security have to do what the partners want, even if it's a violation of policy and common sense," Nelson adds. "They scream 'I want! I want! I want!' And they get it because they're high up the food chain."

Andrew Jurczyk, chief information officer at Seyfarth Shaw in Chicago, says employee education is the most important part of a security system. "It's extremely important for firms to provide education to their user base," he says. "They need to know what encryption is, and what possible sources [of data leakage] are."

AUDIT TRAILS

To protect their networks on the technical side, firms need to have data leakage prevention tools or internal computer audit trail monitoring, Raul says.

"That will ascertain whether there are any unusual, untoward, suspicious accesses to files, emailing of large quantities of files to personal email accounts, and so on," he says. "There should be automatic encryption of USB drives, and there ought to be limits on who can access what information."

Since firms are perhaps most vulnerable to extrusion when an employee is about to leave, systematic processes are needed to handle that transition, Jurczyk says. "Typically, when somebody is leaving, they go through appropriate channels for the amount of data they're allowed to take," he says. "We produce it for them on a DVD and hand it over. It gets treated as a matter of record, and we go on from there."

Particularly if an employee is disgruntled—and even more particularly if they're being fired—firms need to be on maximum alert, Nelson says.

"Kill their ID, cut their remote access," she says. "There's a whole checklist of things you need to do to make sure there's no further visit to the data by the person you're terminating."

This article originally appeared in the July 2014 issue of the ABA Journal with this headline: "Inside-Out Threat: Law firms' own employees are among the major cyberthreats they must protect against."

Previous:
Soft terms turned to solid tips at Avvo's Lawyernomics 2014 (http://www.abajournal.com/magazine/article/soft_terms_turned_to_solid_tips_at_avvos_lawyernomics_2014/)

Next:
Preparing for the 'Internet of things' (http://www.abajournal.com/magazine/article/preparing_for_the_internet_of_things/)

Filed under:

Law Firms (http://www.abajournal.com/topic/law+firms/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Law Practice Management (http://www.abajournal.com/topic/law+practice+management/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Legal Technology (http://www.abajournal.com/topic/legal+technology/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Business of Law (http://www.abajournal.com/topic/business+of+law/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Business of Law (http://www.abajournal.com/topic/business+of+law/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Cybersecurity (http://www.abajournal.com/topic/cybersecurity/?utm_source=website&

utm_medium=web&utm_campaign=related_topics)

You might also like:

- Citing twin law firm websites (1 real, 1 fake), bar group urges public to beware (http://www.abajournal.com/news/article/bar_group_points_to_twin_law_firm_websites_1_real_1_fake_urges_public_to_ch/)
- Gay 'conversion therapy' for minors opposed by ABA House leaders (http://www.abajournal.com/news/article/gay_conversion_therapy_for_minors_unanimously_opposed_by_aba_house_leaders/)
- Nearly 4 million affected by hack on medical records systems software company, feds say (http://www.abajournal.com/news/article/nearly_4_million_affected_by_hack_on_medical_records_systems_software_compa/)
- US increasingly uses malware in law enforcement, expert says; should a warrant be required? (http://www.abajournal.com/news/article/us_increasingly_uses_malware_in_law_enforcement_expert_says_should_a_warran/)
- Ex-Wilson Sonsini worker who ignored 'wake-up call' insider-trade case gets 2 years (http://www.abajournal.com/news/article/ex_wilson_sonsini_worker_gets_2_years_for_insider_trading_case_against_lawy/)

We welcome your comments, but please adhere to our comment policy (/commentpolicy/). Flag comment for moderator. (/report_abuse/)

Comments

Ahmed Masud said:

Very interesting article. It makes some great points. Indeed, there are a lot of well understood processes that should and can be put in place to ensure safety from disgruntled or exiting employees. The point about education is also well made. Knowledgeable employees will know what not to do by accident.

However IMHO the problem is much bigger than that. For instance, once employees know what not to do they also find out what the vulnerabilities are within the system and how to subvert them.

Law firms are a very weak link when compared to the value of the data they house. When just one file can mean a swing of hundereds of millions of dollars to the right buyer, then subverting a $20 million dollar system by throwing around $2 - $5M at it is a no-brainer.

Cyber security experts have known for years that processes, procedures and education are not the solution they are just a first step. Insider threats and channels through which they can enter permute beyond human capacity to manage. Insider threats require automated systems for real-time squashing. Hopefully, leaders like Andrew Jurczyk will set the right example for the industry.

Posted: Jul 11, 2014 08:05 pm CDT
| Flag this comment for moderation (http://www.abajournal.com/report_abuse/?comment_id=363794)

Commenting is not available in this channel entry.

CYBERSECURITY

Is your firm's phone line secure? If not, a hack attack can cost you big bucks

POSTED OCT 21, 2014 01:00 PM CDT

BY MARTHA NEIL (HTTP://WWW.ABAJOURNAL.COM/AUTHORS/5/)

Image from Shutterstock (http://www.shutterstock.com/pic-6228892.html).

Many small businesses don't realize it, but their phone system may be a potential gateway for hackers.

Large companies that contract for service with major carriers have little to worry about, because sophisticated security systems are in place and customers likely will be indemnified if they fail. But small businesses that use local carriers can be hit with—and expected to pay—tens of thousands of dollars in unexpected charges if a hacker breaks through and rapidly rings up huge bills for high-priced calls, reports the New York Times (http://nyti.ms/1qXgILv) (reg. req.).

That's what happened to the architecture firm operated by Bob Foreman in Norcross, Georgia. Over one weekend in March, a hacker ran up $166,000 in phone charges to three foreign countries, which he and his firm, Foreman Seeley Fountain Architecture, are now disputing. Another $17,000 in penalties for late payment and termination are also now at issue.

Such schemes typically involve a hacker who has leased a premium-rate 900-number phone line, like the ones that are often used by psychic and sex-chat services, the newspaper explains. A caller to one of these lines pays more than $1 a minute, and the lessee gets a percentage of the payments for calls made to the number. If a hacker then breaks into a business' phone network, they can use a high-speed computer to make as many as 220 calls per minute from the business to that 900 number. The hacker's percentage from charges which are then billed to the business can be substantial, according to the Times.

Credit card companies are required by law to reimburse their customers for fraudulent charges, but phone carriers have no such obligation under current federal regulations. Thus, their customers are left unprotected. Last year alone, reports the Times, the global cost to victims of these swindles was $4.73 billion.

Turning off call-forwarding and setting strong passwords for voicemail can help prevent other

businesses from being victimized, recommends Jim Dalton of TransNexus. His company sells Internet calling-management software.

“People don’t realize their phone is a six-figure liability waiting to happen,” he told the Times.

Previous:
Woman's condo is sold at auction because of $95 overdue tax bill; she says she never received notice (http://www.abajournal.com/news/article/womans_condo_is_sold_at_auction_because_of_95_overdue_tax_bill_she_says_she/)

Next:
As fewer law grads become lawyers, the profession shows its age (http://www.abajournal.com/news/article/as_fewer_law_grads_become_lawyers_the_profession_shows_its_age/)

Filed under:

Media & Communications Law (http://www.abajournal.com/topic/media+communications+law/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Consumer Law (http://www.abajournal.com/topic/consumer+law/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Law Practice Management (http://www.abajournal.com/topic/law+practice+management/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Legal Technology (http://www.abajournal.com/topic/legal+technology/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Business of Law (http://www.abajournal.com/topic/business+of+law/?utm_source=website&utm_medium=web&utm_campaign=related_topics) | Cybersecurity (http://www.abajournal.com/topic/cybersecurity/?utm_source=website&utm_medium=web&utm_campaign=related_topics)

You might also like:

- Citing twin law firm websites (1 real, 1 fake), bar group urges public to beware (http://www.abajournal.com/news/article/bar_group_points_to_twin_law_firm_websites_1_real_1_fake_urges_public_to_ch/)
- Gay 'conversion therapy' for minors opposed by ABA House leaders (http://www.abajournal.com/news/article/gay_conversion_therapy_for_minors_unanimously_opposed_by_aba_house_leaders/)
- Nearly 4 million affected by hack on medical records systems software company, feds say (http://www.abajournal.com/news/article/nearly_4_million_affected_by_hack_on_medical_records_systems_software_compa/)
- US increasingly uses malware in law enforcement, expert says; should a warrant be required? (http://www.abajournal.com/news/article/us_increasingly_uses_malware_in_law_enforcement_expert_says_should_a_warran/)
- Ex-Wilson Sonsini worker who ignored 'wake-up call' insider-trade case gets 2 years (http://www.abajournal.com/news/article/ex_wilson_sonsini_worker_gets_2_years_for_insider_trading_case_against_lawy/)

We welcome your comments, but please adhere to our comment policy (/commentpolicy/). Flag comment for moderator. (/report_abuse/)

Comments

BMF said:

Hackers aren't the only issue. A lot of these chat lines are initially accessed by 800 or other toll free numbers. When I worked with disabled adults they often lived in situations where they were given phones that accessed local numbers and 800/toll-free numbers. Contrary to popular belief, they are also sexually aware--but also trusting, and often had no concept of "scams." They were victimized by the chat lines--often to the tune of thousands of dollars per month. AT&T refuses to provide service that allows individual payors to block access to these

900 numbers.

Posted: Oct 22, 2014 10:42 am CDT
| Flag this comment for moderation (http://www.abajournal.com/report_abuse/?comment_id=380215)

Commenting is not available in this channel entry.

CYBERLAW, PRIVACY

What Do Lawyers And Celebrities Have In Common?

By JOSHUA LENON

/ Mar 24, 2015 at 4:44 PM

Besides their good looks and fame, they're also increasing their focus on data security. In the wake of "Celebgate," the Sony Pictures hack, and nearly daily data breaches targeting massive corporations to individuals, law firms are finally recognizing the importance of bringing their cybersecurity policies up to speed.

MENU

encourages lawyers to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable (and emerging) ethical and legal obligations. The cybersecurity program should also be tailored to the nature and scope of the organization and the data and systems to be protected.

A program for cybersecurity is desperately needed in law firms. In the ABA's 2014 Technology Survey, 13% of law firms had suffered a security breach in their IT, and another 25% could not tell if they had a breach. Close to 45% of firms had computers infected with spyware. Law firms have become easy targets for computer hackers due to lax investment in technology and IT personnel, poor understanding of security best practices, and fragmented self-regulation.

Clients are noticing that their confidential information may not be safe with law firms. In the "2014 U.S. State of Cybercrime Survey" by PricewaterhouseCoopers, 59% of respondents said they were more concerned about cybersecurity this year than in the past. Recently, big banks have begun subjecting outside law firms to security audits before entrusting case files to them. This was after the superintendent of New York state's Department of Financial Services sent a letter to dozens of banks requesting information on security risks relating to law firms and other third parties. Law firms working for these banks now have to invest in technology and software upgrades, document compliance procedures, and hire staff to maintain systems and train lawyers and employees on minimizing risks.

For large law firms and celebrities alike, cybersecurity compliance is now a business necessity.

Boutique law firms will also be feeling the need for cybersecurity compliance soon.

Regulations are starting to impose duties relating to the storage and processing of private information on many industries, with lawyers being caught up in these new rules. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the uses and disclosures of protected health information maintained and transmitted by covered entities. Law firms that have protected health information in their case files, due to working with a covered entity, must use "appropriate safeguards" for the protected information as a contracted business associate. If you are a lawyer handling personal injury cases, worker's compensation claims, veteran's affairs claims, and Social

MENU

Real estate law is another practice area having to adjust to new cybersecurity compliance regulations. The Consumer Finance Protection Board issued Bulletin 2012-03, requiring "supervised banks and nonbanks to have an effective process for managing the risks of service provider relationships." This means that mortgage lenders must now monitor their third party vendors' compliance with federal consumer financial laws. In response to this regulation, the American Land Title Association (ALTA) created a system of best practices that it advises real estate closing lawyers and title companies to implement. The ALTA Best Practices document recommends that firms adopt and maintain a written privacy and information security program to protect non-public personal Information as required by local, state, and federal law. If you are a law firm handling housing escrow funds or a title company that does the same, you may now have a cybersecurity compliance burden if you want to work with lending banks.

In addition to industry regulations, states are beginning to enact data privacy laws. California continues to lead the nation with an expansive data breach law, protections for the personal data of K-12 students, and a new law giving minors a limited "right to be forgotten" in the online realm. For law firms that operate in California or process its residents' personal information, keeping compliance with California's growing body of privacy law is a necessity.

With this growing body of statutes and regulation, a lawyer's duty of confidentiality is now extending beyond an ethical obligation enforced by bar associations. Protection of client data now has many enforcers and potential pitfalls abound.

Law firms should begin looking at their activities surrounding their data and the technology that they use to access it. Each firm should undertake a data audit to identify and close vulnerabilities and enact policies to prevent new ones from emerging.

Such policies include:

- Maintaining up to date technology and software;
- Utilizing logging tools and reviewing them frequently;
- Undertake employee training on two-factor authentication, clean desk standards, and strong passwords; and
- Quarterly resets on passwords and technology authorizations.

MENU

Law firms wanting to learn more about practices for protecting their email threads, client data, and "confidential" pictures are welcome to join the seminar, Cybersecurity for Law Firms, where these policies, NIST cybersecurity standards, and issues of cybersecurity insurance will be discussed.

Joshua Lenon is the Lawyer in Residence at Clio, an intuitive cloud-based legal practice management solution. An attorney admitted to the New York Bar, Joshua brings legal scholarship to the conversations happening both within Clio and with its customers. He can be reached at joshua@clio.com.

TOPICS

Advertising, Biglaw, Clio, Cybersecurity, Joshua Lenon, Privacy, Shameless Plugs, This Is an Ad

POPULAR ARTICLES

MENU

Managing Editor
David Lat

Editors
Staci Zaretsky
Joe Patrice

Breaking Media Editor at Large
Elie Mystal

MENU

ABOVE THE LAW

ATL HOW APPEALING

ABOVE THE LAW REDLINE

BREAKING DEFENSE

BREAKING Energy

BREAKING GOV

DEALBREAKER

FASHIONISTA

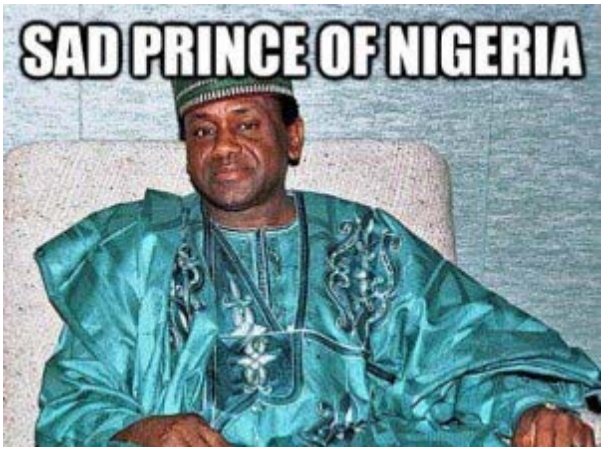
MedCity News

CYBERLAW, INSURANCE, INTELLECTUAL PROPERTY

When Luddites Handle Cyber Security, You End Up With American Law Firms

By JOE PATRICE

13 Comments / / Feb 6, 2013 at 12:50 PM



MENU

Cyber security is all the rage this week, with President Obama announcing that he's working on a new cyber war plan and the Internets freaking out that the Super Bowl blackout was really a Chinese hacking effort.

Some of you probably assume the ATL front page was hacked this week. Don't worry though...we made all those problems ourselves.

Cyber attacks on U.S. businesses have increased dramatically as savvy hackers look to steal financial and intellectual assets from computer systems. The smartest cyber criminals have even figured out the best way to get what they want is to avoid the target corporation entirely and aim straight for their law firm — the soft underbelly of American cyber security...

And for good reason, while corporate America and the military contemplate advanced security systems and detailed retaliation plans and elaborate encryptions, law firms are still falling for the Nigerian Prince scam at an alarming rate. And sometime soon, this is going to turn into a major legal liability for some poor firm.

Don't law firms know that Nigeria doesn't have princes?

I guess we shouldn't be surprised by an industry that thinks "Africa" is a country.

OK, Nigeria has the Kano Emirate...that's a *kind* of royal family, but you know what I mean.

Let's face it, lawyers aren't the most technologically savvy bunch. It's not uncommon for firm leadership to harbor one or two partners who still have their emails printed out for them and then dictate their responses to a secretary. The idea that a massive investment in the firm's technological infrastructure and constant monitoring boggles their mind.

And hackers have figured this out. Probably from Boston Legal reruns. Some, like Joseph DeMarco are blaring the warning klaxon for corporate counsel.

> "The challenge for general counsel is to first understand the magnitude of the threat, the persistence of it, and the fact that it is not only directly against their company, but also indirectly through the company's outside consulting companies, accountants, and lawyers," he told CorpCounsel.com Monday.

MENU

firms that the company consults with, such as its law firms. He calls them "downstream victims."

The George Spelvin Pirate Virus is particularly dangerous

When you think about it, this is painfully obvious. Law firms handle oodles of corporate secrets on often antiquated computer systems. The threat is particularly acute at small firms without the resources for IT departments or constant upgrades. If you're still running Windows 95, you just might have a problem.

Meanwhile, hackers have become so complex they can completely commandeer smartphones with one careless click of a fake software update. The FBI keeps a very helpful list of the e-scams on its radar at any given moment. It's worth perusing and then spending an hour in sheer terror that you've already unwittingly sent your client's patent designs overseas.

But cyber attacks, like most events in this country, can spawn lawsuits — against the victims. Craig Newman and Daniel Stein of Richards Kibbe & Orbe warn:

> "With cyber attacks on the rise, prosecutors, regulators, and the plaintiffs' bar are all gearing up to hold corporations responsible for the inevitable losses caused by cybercriminals. And, with more confidential information, including trade secrets and other competitively sensitive material, flowing through the Internet to corporate servers and even to the cloud, the risks for corporate America increase each day. In fact, for every reported cyber attack, experts estimate that there are an additional 100 attacks that are never even detected.

> challenges. Even more unsettling is the large number of scenarios in which a corporation is vulnerable to such risks, and the range of individuals and businesses that may be entitled to take legal action.

And all this liability will trickle down to the law firm identified as the source of the leak.

Insurers are creating new policies to protect law firms from third party liability claims arising from getting hacked and losing client data, but a lot of firms haven't gotten the clue yet.

> "Cyber coverage at law firms "is a huge hole right now," says Jim Rhyner, worldwide specialty E&O product manager and specialty law firm practice leader for the Chubb Group of Insurance Cos. in Warren, N.J. "There's a lot of education going on in the marketplace right now about what the exposures are and how to protect against them."

Well that's super. I'm often skeptical of insurance companies explaining how essential an insurance policy may be, but this time I'm pretty sure they're right. If you have any influence over your firm's insurance coverage, you should probably look into this before the hackers knock down your 10-year-old firewall.

And while you're at it, maybe improve that firewall.

New E-Scams and Warnings [FBI]
Calling General Counsel to the Front Lines of Cybersecurity [Corporate Counsel]
Trial Attorneys on Cyber Attacks [Regulatory Cyber Security: The FISMA Focus IPD]
Cyber Liability Emerging As Top Concern In Lawyers' Professional Liability Market [National Underwriter]

TOPICS

Cyberlaw, FBI, Insurance, Intellectual Property, Nigerian Scams

MENU

13 comments

(hidden for your protection)

SHOW ALL COMMENTS

Subscribe and get breaking news, commentary, and opinions on law firms, lawyers, law schools, lawsuits, judges, and more.

Contact Us

Tips and General Inquiries

email
tips@abovethelaw.com

text message
646-820-8477

Advertising Inquiries

advertising@breakingmedia.com

Editorial Staff

Managing Editor
David Lat

Editors
Staci Zaretsky
Joe Patrice

MENU

OUR SITES

ABOVE THE LAW

ATL HOW APPEALING

ABOVE THE LAW REDLINE

BREAKING DEFENSE

BREAKING Energy

BREAKING GOV

DEALBREAKER

FASHIONISTA

MedCity News

4 Ways You Are Putting Your Clients' Information at Risk

By Sam Glover on May 19th, 2015

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. (Rule 1.6(c).)

So what are *reasonable efforts* when it comes to your clients' information stored on your computer? You have to make *an* effort, obviously. But how much effort is so unreasonable that you don't have to make it?

At a minimum, a reasonable effort has to mean taking advantage of the easy-to-use security features already available on your computer and device(s). Where the potential harm is great and the potential fix is cheap and easy to implement, it is also be a reasonable effort.

With that in mind, here are four ways you may not be making a reasonable effort.

1. You Don't Encrypt Your Clients' Files

If you are using a Mac or a Windows PC that has Bitlocker, you can encrypt your files with just a few clicks. That is not hyperbole. All you have to do is change a setting.

But is it reasonable? Well, after you encrypt your computer and devices, you can continue using them exactly as you do now. And while encryption will affect your computer's performance, the change will be so small that you aren't likely to notice. Encrypting your files barely takes any effort, so it must be reasonable.

Many lawyers misunderstand what encryption means for using their computers. Under Rule 1.1, they probably have a duty to be better-informed about encryption technology, but the bottom line is that after encrypting your computer you can go on using it exactly as you do now. It is not like email encryption, which definitely still is pretty clunky. You can open and save files, send and receive files, and generally go on using your devices just like you are used to.

You should definitely be encrypting your client files.

2. You Don't Use a VPN

When you use a strange Wi-Fi network, it doesn't matter whether you have to log into that network with a password or not. It is, for all intents and purposes, public. And *public* means that when you browse the web or check your email, you might as well be sharing it with the room. Anyone who wants to listen in, can. It isn't even illegal. If you send a confidential document as an email attachment over a public network, anyone can read it.

Keeping your Internet activity private is not difficult or expensive, but it does require you to use a third-part service called a VPN (**v**irtual **p**rivate **n**etwork). A VPN is a secure line to the web that prevents anyone on the same network from seeing what you are doing online. As Kashmir Hill recently said, "if you use the Internet, you need a VPN."


Tips You Need to Start Using (Sponsored)


Podcast #28: Nicole Bradick on How to Build a Virtual Law Practice


Best Law Firm Websites, 2014 Edition


Why Are Lawyers So Expensive? I'll Tell You Why


Proper Deposition Objections


NeatDesk Desktop Scanner: Don't Try Neat?


Fashionable, Professional Bags for Women Lawyers

3. You Don't Use Two-Factor Authentication for Key Services

Two-factor (sometimes called two-step or multi-factor) means using something you know (your password) and something you have (usually your phone) to log into an account. With two-factor authentication, you have to type in your password plus a code generated by an app or sent to you by text or email. Two-factor authentication is slightly more work than logging into your account with just a username and password, but it is also drastically more secure. Even if a malicious hacker has your username and password, they will not be able to log into your account or reset your password unless they also have access to your phone.

Without two-factor authentication, anyone who cracks your password can access your accounts. And anyone who gains access to your email account can change the passwords to all your other accounts, which will let them empty your bank accounts (goodbye, client funds!), go on a shopping spree on Amazon, or if you are lucky, turn your computer into a spambot.

If you aren't using two-factor authentication on your critical accounts, you aren't making reasonable efforts to protect the client information stored in *any* of your accounts.

4. You Don't Use Good Passwords

Good passwords may be the last thing on this list, but they are the most important, without a doubt. Even if you take all the precautions in the world, they won't do any good if you use weak passwords.

Last year, Russian hackers acquired 1.2 billion passwords. If each of those passwords represents a person, that means the hackers compromised about 17% of the world's population. In order to get those passwords, they will have to attempt to decrypt the passwords. This is not particularly difficult.

If your password in the dictionary or uses common substitutions like `1` for `l` or `@` for a, it will only take seconds to decrypt your password. If you use a long, randomly-generated password, it may be effectively impossible to decrypt. If your password is somewhere in the middle, cross your fingers and hope the cracker gets bored before it brings the necessary processing power to bear.

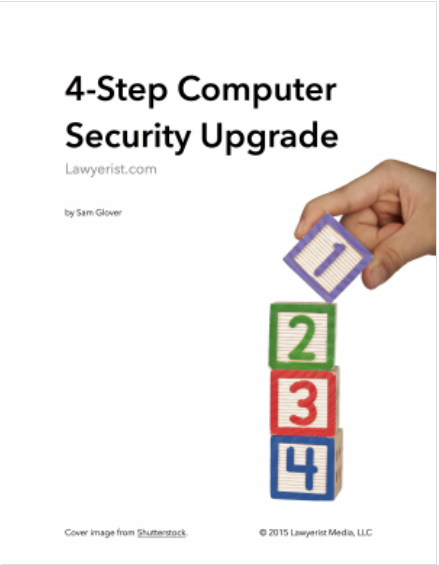
If a hacker manages to get ahold of your username or email address, connected with your password, then that hacker can access any other account for which you use the same credentials. In fact the first thing they will probably do once they have your credentials is try them on a list of popular websites.

Using good passwords is not unreasonable, it is required.

Fix These Things Now

A few months ago, Aaron and I put our heads together to try to identify several things lawyers could do to drastically improve their computer security. We identified each of the problems listed above.

If you aren't doing any of these things, we would give you a D- when it comes to your own computer security. But you can fix all of these things in under an hour (or start, in the case of using good passwords). All you need is a step-by-step guide to doing each of them.



I spent the last couple of months putting together a step-by-step guide to doing just that. You can get the "4-Step Computer Security Upgrade" right now.

It won't make your computer impregnable, but it will upgrade your computer security from a D- to at least a solid B. If you get the guide and follow the instructions, you can rest easier knowing you have taken care of the low-hanging fruit and made your computer far more secure than it was.

Featured image: "Umbrella in the rain in vintage tone" from Shutterstock.

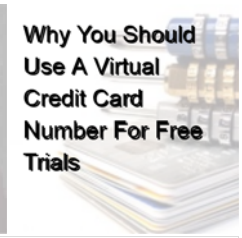
Legal Ethics, Legal Technology

data security, Lawyerist Survival Guides, security, tech competence, white papers

Sam Glover is a writer, speaker, lawyer, and the founder of Lawyerist. Sam writes, speaks, and podcasts about legal technology, law practice management, marketing, and more. His most recent publication is Lawyerist's "4-Step Computer Security Upgrade."

@samglover
samglover.net

MORE FROM ISSUE #21



READ THE FULL ISSUE