Ethical and Legal Obligations for Confidential Data

Ethical Obligations

Competent representation and confidentiality are at the foundation of the attorney-client relationship. ABA Model Rule 1.1 and Florida Rule 4-1 covers the general duty of competent representation and provides that "Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." ABA Model Rule 1.6 and Florida Bar Rule 4-1.6 generally defines the duty of confidentiality—and it extends that duty to "information relating to the representation of a client." It's now commonly accepted that this duty applies to client information in computer and information systems as well.

In addition, Model Rule 1.6, Comment 18 requires reasonable precautions to safeguard and preserve confidential information (a similar comment is located after Florida Rule 4-1.6):

> 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.

Common Law Duties

Along with the ethical duties described, there are parallel common law duties. The Restatement (3rd) of the Law Governing Lawyers (2000) summarizes this area of the law. *See* Section 16(2) on competence and diligence, Section 16(3) on complying with obligations concerning client's confidences, and Chapter 5, "Confidential Client Information." Breach of these duties can result in a malpractice action.

There are also instances when lawyers may have contractual duties to protect client data. This is particularly the case for clients in regulated industries, such as health care and financial services, that have regulatory requirements to protect privacy and security.

Laws and Regulations Covering Personal Information

In addition to the ethical and common law duties to protect client information, various state and federal statutes and regulations require protection of defined categories of personal information. *See* 19 C.F.R. § 201.6; Fla. Stat. §§288.075, 501.171.

Standards for Competent and Reasonable Measures

The core challenge in establishing information security programs is deciding what security measures are necessary and then implementing them. Determining what "competent and reasonable measures" are can be difficult. Legal standards that apply in other areas, like financial services, can be helpful in providing a framework, even though they do not legally apply to the practice of law. The requirements in the rule, Standards for Safeguarding Customer Information, 16 C.F.R., Part 314, provides a short yet comprehensive list of the components of a complete security program.

Articles and Reference Materials for Cybersecurity

*Complete PDF's will be on the Inn of Court website

- Jonathan Baker, Flying in the Clouds: Practicing Law by Cloud Computing, 85 Fla. B.J., 9 (Nov. 2011).
    - Tips on cloud computing and how law offices can reduce the risks of unauthorized users accessing confidential client information when information is stored on the cloud.
- Ed Finkel, *Client Confidentiality in the Digital Age*, 103 Ill. B.J. 20 (May 2015).
    - Common mistakes lawyers when receiving, accessing, and using client information.
- Shaun Jamison, *Your Money or Your Data*, 73-SEP Bench & B. Minn. 24 (Sept. 2016).
    - Defining ransomware and how to respond to ransomware attacks.
- Edward J. McAndrew, *The Data Security Imperative for Lawyers*, 32-FALL Del. Law. 30 (Fall 2014).
    - List of data security leading practices and core concepts such as data retention and destruction, electronic communications, and cloud services.
- Karen P. Randall & Steven A. Kroll, *Getting Serious About Law Firm Cybersecurity*, 300-JUN N.J. Law. 54 (June 2016).
    - Summary of law firm cybersecurity breaches in the news, ethical obligations for lawyers, and analysis of liabilities law firms face from top cyber threats.
- tmgroup, *How to Prepare to Defend Your Law Firm's Reputation in the Event of a Cyber-Attack*, Lexology (Nov. 21, 2016), http://www.lexology.com/library/detail.aspx?g=36b42e78-d97e-40ae-9032-7a359eb524e5&l=7TXDE6U.
    - How to create a cybersecurity communication plan in response to a cybersecurity breach.
- Legal Service Information Sharing and Analysis Organization (LS-ISAO) – Industry Best Practices
    - The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an organization dedicated to providing resources for cybersecurity practices to their members in the financial industry. Their website contains helpful "industry best practices" guidelines and forms which can also be applicable to law firms. Examples include security tips on how to secure a mobile device or computer, and how to communicate to employees or others on how to reduce the risk of cyber attacks.
- Industry Best Practices Forms – https://www.fsisac.com/news/industry_best_practices.

The Florida Bar Journal

Advertising Rates • Submission Guidelines • Archives • Subscribe • *News*

November, 2011 Volume 85, No. 9

Journal HOME

Flying in the Clouds: Practicing Law by Cloud Computing

by Jonathan Baker

The issue of this article is this: What can a law office do to reduce the risks of improper access to its clients' confidential information when that information is stored via cloud computing?

But first, what is cloud computing? Cloud computing is best described as connecting your home to the electricity of a power plant instead of using one's own candles.[1] Put another way, cloud computing is analogous to connecting a home to a city water supply when previously that home drew its water from a private, individual well.[2] In cloud storage, a user receives a product by a common grid to which all the other users in the city (cloud) might have access.[3] However, in cloud computing, a neighbor can effectively travel through the pipes and arrive in your kitchen. Such a person could be anyone with access to the Internet, from a person in a nearby coffee shop to an overseas criminal organization.

Technically speaking, cloud storage is the keeping of one's information on another entity's server. Of course, that server is located in a different physical location. In addition, such a system is designated a "cloud" because it consists of a lump of every customer's information, whoever those customers may be. Yet there are no technical barriers separating the information of the various customers.[4] Information can be placed on a particular cloud server from any computer with Internet access; the user does not need a computer equipped with a hard drive. Thus, when a lawyer wishes to access the information previously stored via cloud computing, he or she merely goes to the website of the cloud service provider with the proper username and password.

Similarly, cloud computing allows firms to equip their office computers with the bare minimum software because the server and database of the cloud service provider does the heavy lifting elsewhere. For example, Gmail, Google Docs, and Yahoo!Mail are some common examples of cloud computing. No hard drives are needed to access these applications.

The benefits of having another person bear the energy and space costs of digital storage are stupendous. Cloud technology allows many persons to work on the same document, saving their changes to a master copy, which is stored via cloud computing. This avoids the hassle of multiple copies being exchanged during the revision stage.

What are the risks of cloud computing? Simply put, they stem from breaches in a client's confidential information entrusted to the attorney. Of course, the purest risk is that an unknown party may gain access to a lawyer's digital information while that information is stored on a third party's cloud servers, whoever or wherever that infiltrator may be. Such unauthorized access could be granted either by the negligent or intentional act of a cloud service provider's employee. "Even if a user . . . knows that data is stored in the cloud, it might not be clear exactly where the data is stored."[5] This statement by Professor Felton of Princeton University expresses the first risk that a lawyer may face when using cloud computing: There is little traceability of the location at which one's documents are stored. Specifically, cloud computing generates many backups of any document stored on the cloud system. This can be a blessing and a curse as we shall see. Therefore, one document might be stored in 16 different locations, some of which may be politically unstable nations.[6] The international nature of security breaches is indeed real. Even a U.S. congressman recently noted that foreign governments such as China at times have breached the digital security of the House of Representatives.[7]

A further risk is that the license agreement may allow the cloud service provider to share a specific document with anyone who collaborated with your office to produce it.

In that case, why ever store information by cloud computing? Cost savings is the answer. The federal government projected that employing cloud computing could save 2 to 99 percent of its computing costs in 2010.[8] Likewise, David Barratt, a digital media graduate from the University of Central Florida and head of the web development team at Relevant Media Group in Orlando states: "Cloud storage services are usually more reliable than . . . a server in your office[.] . . . Most offices do not keep off-site backups. This can lead to huge problems if an office hard drive fails. . . . Most cloud services keep off-site backups."[9]

To attempt to answer our issue, the following ideas suggest technical and practical ways for a law office to reduce the chances that an intruder may access confidential cloud data. Some of these suggestions are novel, while some are merely extensions of current procedures.

First, firms should leverage market reputation. In other words, they should perform research on the various cloud computing service providers and choose the one with the best record of security. Cloud service providers are like law firms; they need good reputations to stay in business. Since a cloud service provider likely does not owe many contractual duties to a customer, one way to make providers change their standards might be to purchase their competitor's product. A more unified approach to this suggestion would be for The Florida Bar to provide a list of the most proven and secure cloud service providers as confirmed by the law firms who use them. Even Barratt agrees when he says, "A secure cloud is possible if a company is willing to have the title of being the most secure. It is a free market economy that keeps our data private."[10] On top of this, a ranking officer of Salesforce.com stated before the U.S. House of Representatives that his organization hosts a website that daily expresses its cloud system's performance along with the trust its users have grown to feel.[11] Any positive business characteristics like these will likely motivate cloud service providers to create new security measures.

Yet, the market is never perfect. If an office learns its confidential data was breached, the firm should lock its computers so that they cannot be further used to store data on the cloud servers.[12] After confirming that security is regained, the firm can reauthorize its computers to store data in the cloud.[13] During this lockdown, office workers can use hard drives or flash drives for storage.[14] This suggestion is feasible because cloud service providers record the time at which a document is accessed from the cloud server. In parallel to the free market concept, cloud service providers are likely to tell the consumer when its document is infiltrated because keeping a watchful eye on a customer's data is likely a coveted market characteristic. Incidentally, this lockdown procedure is based on a template of the U.S. government's system of digital security, which is known as the Federal Risk and Authorization Management Program (FedRAMP).[15]

Another such FedRAMP procedure consists of password protection.[16] FedRAMP recommends a specific document be password-protected and made known to only certain employees based on their positions within the office.[17] In our case, this may include roles such as partner or primary case worker. In addition, all the data stored on the cloud should be encrypted as a security measure.[18] According to Barratt, even the connection between the firm's computers and the cloud service should be encrypted; this should be done with a 128-bit secure socket layer.[19]

An extended feature of password protection includes password difficulty. An employee who has access to cloud computing, like any other sensitive matter, should have a rock-solid password.[20] It is recommended that passwords be changed monthly and that they include numbers, symbols, and capital and lower case letters.[21]

The more complexity, the better the security. Recently, the U.S. chief information officer suggested by its endorsement of FedRAMP that an employee be required to input specific characteristics of the machine that he or she uses in order to access a document.[22] For example, these input requirements could include the machine's name, owner, serial number, manufacturer, geographic location, software license, network address, or model.[23]

Obviously, the more often cloud activities are monitored, the more secure they are. Barratt suggested based on the current practice of some banks, namely whenever a user from an outside location attempts to access the office's cloud account, the owner of the account is sent a text message.[24] Then the owner must respond with a text message containing a code or password in order for the requesting user to even access the cloud account. In this way, a person in Venezuela cannot access confidential documents without confirmation from home base in Florida.[25]

On the bright side, redundancy may be a firm's friend. Sometimes in an office, security clearances can overlap. For example, Department A creates a spreadsheet and imposes one form of general security in order to view the document while Department B of the same office later inserts a specific authorization requirement in order to view a certain cell of that document. Whereas usually the more security procedures an office employs, the less efficient it becomes, when authorization requests are compounded in the same document, cloud computing security can increase. For this reason, the U.S. Office of Citizen Services and Innovative Technology considers prior authorizations imposed into a document to be positive leverage for cloud security.[26] In this way, security can be increased when many departments contribute to the same document, each imposing its own form of authorization for the section that it contributed.

Beyond the technicalities, the practical suggestion is this: An office should train its staff to securely navigate within the cloud. Once an office has formed a cloud-savvy staff, regular audits are a wise way to ensure the office's internal compliance.[27] Likewise, office security would be more efficient if a cloud computing specialist were appointed within the firm's department of office management, given that the office possesses this level of sophistication. For instance, a cloud computing specialist could recognize the potential security issues posed by the habits of employees. A specialist on staff could also be the innovator on behalf of the office who saves the partners the time of having to read articles such as these.

On top of this, all members of an office must act in unison regarding the policy on cloud security. In assessing cloud computing risks, the U.S. General Services Administration stresses that an office should act as a unit when handling issues of cloud security.[28] Of course, teamwork itself is not novel. Yet, because an office is one body made of several parts, it is advisable to express to employees the expectation that they communicate together by encouraging each other to avoid the risks. The good news is that many new employees may also be young and technologically astute and, therefore,

already attentive to the risks of cloud computing. If so, the costs of implementing a policy through a specific cloud computing division will likely be absorbed more quickly.

The point of these practical suggestions — appointing a specialist, auditing, and actively encouraging teamwork — is simply to say that the risks of cloud computing are best vaccinated when they are met deliberately. Consider it as valuable as the proper accounting of taxes, trust accounts, and other risk management in the practice of law.

In conclusion, your office may find that cloud computing presents benefits that are too large to forego simply because of the risks. Thus, the risks can and should be addressed by a law firm via an information technology expert. That person would do well to employ a progressive strategy that includes some of the suggestions mentioned here, both technical and practical. The progressive nature of technology, as well as the economic impulse of persons who would breach the security of cloud computing, compels a proactive approach. Surely a sophisticated wrongdoer does not have his head in the clouds, and neither should a contemporary law office.

[1] *Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud*: *Hearing Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform*, 111th Cong. 11 (2010) (statement of Vivek Kundra, Fed. Chief Information Officer for E-Government and Information Technology, Office of Management and Budget).

[2] *Id.*

[3] *Id.*

[4] Telephone interview with David Barratt, head of web development team, Relevant Media Group (May 29, 2011).

[5] *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 15 (2010) (statement of Edward W. Felten, professor of computer science and public affairs, Princeton University).

[6] Jonathan Strickland, *How Cloud Computing Works*, http://computer.howstuffworks.com/cloud-computing.htm (play audio file “The Dark Side of Cloud Computing”).

[7] *Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud*: *Hearing Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform*, 111th Cong. 6 (2010) (statement of Rep. Darrell Issa, member, H. Comm. on Oversight and Government Reform).

[8] *Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud*: *Hearing Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform*, 111th Cong. 5 (2010) (statement of Rep. Edolphus Towns, chair, H. Comm. on Oversight and Government Reform).

[9] Email from David Barratt, head of web development team, Relevant Media Group to author (May 18, 2011) (on file with author).

[10] *Id.*

[11] *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 39 (statement of David Schellhase, executive vice president and general counsel, Salesforce.com).

[12] FedRAMP: Control Tailoring Workbook, 1-4 (Oct. 18, 2010) (FedRAMP_Control_Tailoring_Workbook_Template.pdf *available within* https://info.apps.gov/sites/default/files/FedRAMP-Templates.zip).

[13] *Id.*

[14] *Id.*

[15] CIO.GOV — Federal Risk and Authorization Management Program (FedRamp): Introduction, http://www.cio.gov/pages-nonnews.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP.

[16] FedRAMP: Control Tailoring Workbook, 4 (Oct. 18, 2010) (FedRAMP_Control_Tailoring_Workbook_Template.pdf *available within* https://info.apps.gov/sites/default/files/FedRAMP-Templates.zip).

[17] *Id.*

[18] *See* email from David Barratt to author, note 9.

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] FedRAMP: Control Tailoring Workbook, 10 (Oct. 18, 2010) (FedRAMP_Control_Tailoring_Workbook_Template.pdf *available within* https://info.apps.gov/sites/default/files/FedRAMP-Templates.zip).

[23] *Id.*

[24] *See* email from David Barratt to author, note 9.

[25] *See* telephone interview with David Barratt, note 4.

[26] *Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud*: *Hearing Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform*, 111th Cong. 32 (2010) (statement of David McClure, associate administrator, Office of Citizen Services and Innovative Technologies, U.S. General Services Administration).

[27] FedRAMP: Control Tailoring Workbook, 10 (Oct. 18, 2010) (FedRAMP_Control_Tailoring_Workbook_Template.pdf *available within* https://info.apps.gov/sites/default/files/FedRAMP-Templates.zip).

[28] *Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud*: *Hearing Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform*, 111th Cong. 24 (2010) (statement of David McClure, associate administrator, Office of Citizen Services and Innovative Technologies, U.S. General Services Administration).

Jonathan Baker *is a third-year law student at the Florida State University College of Law. He is the winner of the 2011 essay writing contest for Florida law students sponsored by Florida Lawyers Mutual Insurance Company and the Young Lawyers Division of The Florida Bar. The contest topic was "best practices for a law office in the age of cloud computing."*

This article was originally printed in the Florida Lawyers Mutual Insurance Company's newletter, Advisor*, and is reprinted with permission.*

This column is submitted on behalf of the Young Lawyers Division, Sean Timothy Desmond, president. William E. Loucks, president of FLMIC, Judge Bob LeBlanc, and Renee E. Thompson were judges of the contest.

[Revised: 02-10-2012]

Journal HOME

Working at the Bar
Contact Us
Diversity
Leadership Academy

Issue Papers
Publications

Unlicensed Practice of Law
Lawyer Referral Service

Legislative Activity
Lawyer Referral Service
Voluntary Bar Center

Courts and Judges
Legal Groups and Law Schools
Judicial Nominating Commission

103 Ill. B.J. 20

Illinois Bar Journal
May, 2015

Article
Ethics

CLIENT CONFIDENTIALITY IN THE DIGITAL AGE

Ed Finkel [a1]

The pathways for breaching client confidentiality - whether due to simple carelessness or inadequate security - continue to multiply as technology advances.

***21 One Illinois attorney responded to a bad review on Avvo in a way that the ARDC said violated client confidentiality. Another uploaded to You Tube a video recording of his client involved in a drug transaction. A third disclosed to the state's attorney that his client had (privately) changed his story in a case to say that he had, in fact, engaged in conduct that resulted in a felony murder charge.**

"There are many recent cases where lawyers have found themselves in trouble because of their use of client confidential information in settings that might surprise people," says Mary K. Foster, counsel to the Attorney Registration and Disciplinary Commission (ARDC) review board and lecturer on legal ethics at Northwestern University School of Law. "They can send unencrypted e-mail. They can use client information gained through conversations with the client, in ways that the client might not anticipate." (Foster will speak on this topic in May - see sidebar on page 22.)

Regarding these types of cases and other confidentiality-related matters - which can be related to the set-up of physical office space, in-office computer networks, and external services like the cloud - attorneys and their firms need to review Rule 1.6 of the Rules of Professional Conduct that covers confidentiality, says Nerino Petro, chief information officer with Holmstrom & Kennedy, P.C. in Rockford and before that a lawyer-technologist with the State Bar of Wisconsin.

"That's kind of the foundation for where we need to begin," he says. "Rule 1.6 applies to conversations we have in public, at the office, in electronic communication, with our data. There are certain levels of protection you can obtain, but then there's another layer of complexity if you're dealing with anything that may be covered by HIPAA or HI-TECH, or federal regulations like FERPA, which may have higher standards than what we may think is necessary based on the Rules of Professional Conduct."

Allison Wood, a former ARDC litigator who's now principal with Legal Ethics Consulting, P.C., sees two main concerns around confidentiality. "Attorneys must be mindful in taking the requisite steps to ensure the protection of client information when they utilize social media, and when they engage in advancing technologies to deliver legal services," she says.

"Breaches most often occur when an attorney sends an e-mail communication to the wrong party; when they post client information on social media without the client's consent; when they leave a laptop unattended and someone steals it or hacks into it; or when office mates leave copies of client documents on the shared copying machine," Wood adds. "There just needs to be a mindfulness in the way the attorney manages his or her practice. They have to think before they post (and) consider their surroundings when they meet clients, or where they will work on client matters."

Errors of commission

Attorneys don't adequately monitor their e-mail and social media behavior in part because they don't understand that electronic communication leaves behind a footprint, Foster says. “I teach my students that e-mail equals ‘electronic eternal evidence,”’ she says. “What you do online, there's a record of it, just as if you were writing a letter to someone or stating it in a court transcript. We've become so accustomed to using the Internet and using these [online] tools, we sometimes use them in situations that violate our client confidences.”

In the example involving the bad Avvo review, the client had complained that the services provided in an employment discrimination case had been inadequate. In her response, the attorney “stated that the client had lost his case because he had engaged in a physical altercation with someone, which wasn't in his initial [Avvo] review,” Foster says.

The ARDC reprimanded the attorney for violating client confidentiality for responding, which “might surprise lawyers, that they can't respond that way,” she says. While an attorney can certainly mount a defense if sued for malpractice, “they can't respond in a more informal setting,” even if the information they disclose is accurate.

In the YouTube case, the defense attorney had received the video recording from the prosecutor and uploaded it with the title, “Cops and Task Force Planting Drugs.” “He claimed he was trying to get a sense of whether the video actually showed the cops planting drugs,” Foster says. “He realized later that it showed the client purchasing drugs.” The client lived in a small town, and when the clip went viral around the town, “she wasn't happy, understandably.” (The attorney challenged ***22** his suspension in federal court - see *Lawyer sues after his YouTube post of client leads to suspension* (LawPulse, May 2014 *Journal*)).

In the felony murder case, the defense attorney initially said his client had an alibi and then disclosed the client's change of story to the prosecutor, which he did not have permission to disclose, yet “argued that he was doing it on behalf of his client,” Foster says. The state's attorney then charged the client with felony murder, and the attorney was found to have violated confidentiality rules. “In all of these cases ... the lawyers didn't necessarily have bad intent ...,” she adds. But they were disciplined nontheless.

Creating secure physical space

Aside from cases in which attorneys take an active role in breaching confidentiality, Foster presents a second set of concerns revolving around errors of omission, starting with both physical and cyber security in-house and extending outward to the cloud.

Regarding physical office space and related firm policies, Foster poses a couple questions that she says attorneys and firms should be asking themselves. “Are hard copy documents secured properly?” she says. “Can client conversations be overheard from the waiting room?”

For Petro, concerns about physical office space boils down to “the little things,” such as “putting files away in your cabinets, not putting your server in open areas - I've seen break rooms where a firm has put their server - and not leaving [computer] passwords lying around.”

Cyber insecure

Lawyers and their firms are vulnerable to cyber attacks precisely because they think they're invulnerable, Foster says. “To most lawyers, this sounds like the stuff of science fiction,” she says. “But it's becoming a real concern. It should

concern most lawyers, not only lawyers in large firms representing corporations in mega-deals but also small firm lawyers because increasingly, these lawyers are becoming targets for hackers.

“In that situation, it's not the lawyer making a judgment error, but being a Luddite and not understanding new technology,” Foster adds. “They can't put their heads in the sand and think they're safe from attack because they're not.”

Attorneys and law firms have become targets for hackers because they maintain a lot of confidential client information in their records, such as financial details and Social Security numbers, often in electronic form, Foster says. “Just like anyone else, just like any other agency that keeps information on behalf of a client, you need to make sure you're securing it properly,” she says. “It isn't so much a disciplinary concern as it is a risk management concern for lawyers.”

Few cybersecurity-related cases have reached disciplinary boards like the ARDC, Foster says, but their potential to cause other kinds of trouble is rampant. “We've all heard about the possibility that the (National Security Agency) listened in on confidential lawyer communications,” she says. “The ABA wrote a letter last year to the NSA about concerns about NSA's use of confidential attorney-client communications, that they might be spying.”

More broadly, “What we're hearing is that it's not uncommon these days for law firms to be targeted by hackers for private information, just like anyone is, just like citizens are,” Foster adds. “While you can never alleviate all possibilities of a breach, you can reasonably protect yourself with some planning.”

External and internal hackers

While intellectual property lawyers and those who handle corporate secrets probably understand the need for strict security measures, “the average lawyer probably spends far less time thinking about data and confidentiality risks,” Foster says. “All lawyers, however, should consider whether their client information is secure, whether it be from a cyber attack, an e-mail scam, or from an errant employee.”

To protect themselves and their firms, attorneys need to ask themselves another series of critical questions, Foster says. Regarding their own computer systems, “Should they encrypt their email? Should they scrub their documents? Should they install [security] systems ***23** in their office to protect client matters?” she says. “Should they rely on outside [security] services? And how do they protect themselves from their own employees? How do they protect their employee information?”

There have been cases where employees have taken confidential information and misused it, Foster adds, and in some of those cases it's been disgruntled or otherwise malevolent departing employees. “They take the laptop,” she says. “What if confidential client information is contained on those laptops?”

That leads to a set of policy questions, Foster says. “Do you allow employees to take home laptops, tablets, or firm cellphones?” she says. “What is your firm policy on the use of cellphones? Do you allow guests and clients to gain access through Wi-Fi while in the office? If so, is it secure? Are your clients' identities protected?”

Attorneys who value their mobility away from the office have to be doubly careful, Wood says. “Generally speaking, the truly mobile attorney has to recognize that meeting with a client in an open public place does not lend itself to a secure confidential exchange,” she says. “Working on a laptop in a coffee shop could create a risk when you tap into the Wi-Fi of the coffee shop, which could mean anyone can see your files.”

System security

Petro mentions some practical steps attorneys and their firms can take to secure their systems against hackers. For one thing, out-of-date hardware and software that's no longer manufacturer-supported makes you vulnerable. “This is where a lot of lawyers fall down,” he says. “This is not a secure operating system. You're going to have to keep your technology up to date.”

Attorneys and firms also need anti-virus, anti-malware, and firewall programming, as well as individual, secure logins and passwords, Petro says. “It's all of these kinds of basic, due-diligence things that people overlook,” he says. “Everybody has to have their own user log-in--not ‘Worker 1’ and ‘Worker 2’ and everybody shares it. They need passwords. Systems need to lock down when they're not at their desk. If a client comes in late, and their kids are running around, and the secretary's work station isn't locked, the next thing you know it has a virus because they're playing on it.”

Passwords need to be changed on a “semi-regular” basis, at least annually, and ideally they should be no fewer than 12 characters, with upper and lower case letters, numbers, and special characters, Petro says. “The problem is, not every website supports that (length),” he says. “But the longer, the better.”

Password manager apps like Last-Pass generate random passwords and assign them to various sites, so that all you need to do is remember your password for LastPass itself. “Otherwise, you can't keep track of everything,” Petro adds.

Cloud-based security

For those using outside contractors to manage their cloud services, Foster has another series of questions: “Have you chosen that contractor carefully? Does the contractor work with other lawyers? Do you know where data is stored? Have you completed an assessment of your risks within the last year? Do you have a system in place to detect a breach of security or a cyber threat? Do you have a plan in the event of breach to remediate the damage? Do you regularly communicate your policies to all firm employees? To clients?”

Illinois does not yet have a governing ethics opinion on using cloud technology, which means that “it comes down to due diligence,” Petro says. He echoes Foster in suggesting that attorneys and firms check out the reputation of possible service providers, find out how they secure data and what steps they take.

But don't be afraid of the cloud, Petro says. “Everybody's like, ‘I can't use the cloud, it's too insecure,”’ he says. “I don't agree with that. You have to take reasonable precautions to ensure the confidentiality and security of your data. You can't guarantee there's never going to be a breach.”

A growing number of attorneys and firms are using cloud-based services, Petro says. “As a profession, we can continue to say, this is what our rules require [and stay away from the cloud],” he says. “The reality is that the rest of the world is passing us by and saying this is acceptable. We're going to have to find some way to live in that world. That's going to be the key.”

Encryption

To keep data in the cloud safe, Petro suggests not using free cloud software like Dropbox, or at least use services like Sookasa or Boxcrypter that encrypt the data you upload into accounts like Google Drive. “Everybody uses Dropbox because it's drop-dead easy to use. I understand that,” he says. “I use Sookasa, which is a paid product, with Dropbox. It's HIPAA and FERPA compliant.”

“You've got to be encrypting your data if you put it out on the cloud, unless your service encrypts the data and you control the key,” Petro adds. “That's the ideal situation,” and SpyderOak is among the services that do so. “At a minimum, you

need to do due diligence, for folks providing the encryption of data, that keys are kept separately from the data and not stored on the same server. [Separate storage] decreases the likelihood that hackers will be able to get at everything."

Aaron Brooks, partner at Holmstrom & Kennedy, says that encryption is perhaps the most useful single security measure one can take and suggests encrypting data at all phases of its existence--at rest, in transit, or at the end of its useful life.

"Encryption at rest refers to protecting the electronic storage medium upon which a unit of information resides. In other words, any place that electronic client information is stored should be properly encrypted," he says. "Thus, laptop computers, tablets, phones, USB drives, and other places that can be used to store client information should be encrypted in a manner that complies with NIST and federal standards for encryption."

Encryption in transit refers to the movement of electronic data from one device to another, Brooks says. "For example, when transmitting data to and from a cloud-based storage service such as Dropbox, one should be able to observe that the browser is connecting via the standard 'HTTPS' secure communications protocol," he says. "Alternatively, when transmitting sensitive information between private networks ... a comparable secure mechanism, such as a VPN connection, should be used."

Finally, at the end of a document's or device's useful life the device used to store electronic client information should be destroyed, Brooks says. "Attorneys can use reputable shredding services to destroy old devices such as hard drives and USB drives, and often these services will provide a certificate of destruction for the file," he says.

Footnotes

a1 *Ed Finkel is an Evanston-based freelance writer.*

End of Document

73-SEP Bench & B. Minn. 24

Bench and Bar of Minnesota
September, 2016

Legal Tech: Embracing the Future

YOUR MONEY OR YOUR DATA

Shaun Jamison [a1]

***25** Trends in other industries make it clear that lawyers must prepare for ransomware attacks. Here's how to get started.

Earlier this year, ransomware cyber attacks at Hollywood Presbyterian Medical Center in Los Angeles, California and MedStar Health, based in Columbia, Maryland, made headlines and alarmed health providers and patients. The ransomware attacks, which involve a virus that is designed to hold data hostage until the victim pays for a "key" to regain access to their data, should also serve as a warning to lawyers.

Indeed, in a recent ransomware case involving the Brown Law Firm in Jacksonville, Florida, the firm was not able to access its client data. [1] Instead, the firm received a message stating that their data was not accessible and it would be destroyed unless the firm paid the equivalent of $2500 in Bitcoins to the hackers behind the attack. Although the firm hired an information Technology (IT) professional, it ultimately decided to pay the ransom on the advice of that IT contractor; the risk of losing the data by attempting to circumvent the ransomware was too great. Such attacks are often successful because the hackers behind the assault ask for a relatively small amount, knowing they can spread fees over many victims. This attack strategy also makes it an easier choice for the lawyer to pay.

WHAT IS RANSOMWARE?

Ransomware is a malicious computer program (also known as malware) that is introduced into a computer system like a virus and allows the attacker to block access to the victim's computer data and demand payment for restoring the data. Typically, there is a time element to the ransom demand: The owners of the data are threatened with its destruction if the ransom is not paid within a predefined number of hours. If you do not represent likely targets of ransomware, does this affect you as an attorney? Yes, because your law firm or corporate legal department is a target.

WHAT IS THE RISK?

Lawyers, just like health and finance professionals, maintain confidential and sensitive information which they are obligated to protect and need to access to serve their clients. Lawyers can be locked out of data, and the data may be sold or made public.

SHOULD I PAY?

This is the big question, and one without a great answer. If you pay, you are likely to get your data back. However, you will be a more likely target in the future and you will unwillingly be funding attacks on other lawyers. Further, there is no guarantee the hackers will honor the agreement. [2] Prevention is ideal, but if you are the victim of an attack, you will

have to evaluate whether you can both restore data and protect against its release without paying the hacker. Ironically, sometimes even the police are left with no better option than paying the ransom.[3] The FBI has sent mixed signals on whether to pay or not, most recently advising against it.[4] Consulting with an IT professional and law enforcement will help you with the decision-making process.

*26 PREVENTING RANSOMWARE ATTACKS

While there is no means of attaining perfect assurance against a ransomware attack, the following precautions can help to mitigate risk and to diminish the impact of a breach on your practice.

• **Good backup:** If you have a backup, you can restore the data to the point of last back up. But you still have a confidentiality issue[5] and the requirement to safeguard client property.[6] You will be obligated to report client data was compromised.

• **Good firewall:** A firewall is the watch guard of the firm's network. Think *of* the firewall as a security bubble. If you turn it on high, you can shut down virtually all communications, but users will complain that system is unusable. If you turn it down too much, you will be open to attack. So you have to find the right balance.

• **Training:** Make sure you and your staff are trained to avoid infecting your network with ransomware. End users can enable breaches by downloading a suspicious attachment or clicking on an unknown link. Hackers use “human engineering” to trick you into clicking on attachments. If you receive a communication that normally would not come by email, do not open the attachment. Call the sender to confirm. Working from home on an unsecured computer can also compromise the network. Network security is only as good as the weakest link. Any device connected to the network needs to be inspected. Educate your staff on how to avoid risks. Use strong passwords and keep them secure. Keep your antivirus software current, but don't assume it is protecting you.

• **Encrypt your data:** This may not prevent an attack, but it will mean an attacker cannot release your clients' confidential data without great effort.

• **Install an ad blocker:** Some ransomware can be delivered via pop-up advertisements.

• **Hire an expert:** Lawyers know what happens when their clients go DIY (do-it-yourself) on complex legal work. Likewise, you should consider hiring an IT professional to evaluate your network's security rather than relying on your own knowledge of cyber security.

• **Use work computers only for work:** Have a computer not connected to your law office network for surfing the internet, or consult your IT professional for other ideas to isolate and protect sensitive areas of your network.[7]

• **Screen and monitor employees:** As noted above, an employee might accidentally open a suspicious attachment or click on an inappropriate link, but in addition some employees might sell your password. According to a recent survey, 56 percent of employees would sell passwords for $1,000 or less.[8]

• **Review your insurance coverage:** Do not assume you have coverage for cyber attacks. Check with your carrier.[9]

*27 DEALING WITH RANSOMWARE ATTACKS

If, despite your best efforts, you become the victim of a ransomware attack, there are several things you will need to do.

• **IT:** Call for IT help, whether internal or an external consultant. Do not undertake any measures on your own unless you are a cyber security expert.

• **Insurance:** Call your insurance carrier. They may be able to help you unwind the problem. And in any case, you may have a notification requirement to secure coverage for an event.

• **Law enforcement:** Call law enforcement.

• **Work your plan:** If you are part of an organization, contact those individuals internally who are identified in your plan, such as partners.

• **Assess the situation:** Can you fix it with a backup.' Was data actually accessed? Is paying a ransom advisable?

• **Determine notification requirements:** Once the attack has been resolved and you are up and running, determine notification requirements. You will want to review the ethics rules as well as any state law requiring notification of a breach. Further, if you have any health data, you may have notification requirements under HIPAA. [10] Failing to disclose, even if you are not required to, may have negative consequences from a trust and public relations standpoint. Weigh your options carefully.

• **Reassess:** Once you are up and running and the system is all clear, take some time to figure out what went wrong and how you can avoid problems in the future.

Ransomware attacks on lawyers are likely to increase. When the Hollywood and Medstar medical data attacks happened, it seemed like the beginning of a trend. Turns out a recent survey shows that half of the hospitals participating in the research had been subjected to ransomware attacks. [11] So the two publicized episodes were public confirmation of a trend, not the possible beginning of one. It may well be the same in the legal industry. Once hackers see success with victims motivated to recover and protect their clients' data, they will continue the attacks as long as it remains profitable. This summer, we learned hackers are targeting lawyers using phony ethics complaints to trick them into downloading an attachment infected with ransomware. [12]

Staying up to date is part of your defense. The ABA's Cyber Security Legal Taskforce is a good source of information. [13] The Better Business Bureau and the FTC have scam alerts. ABA members can also sign up to receive FBI Cybersecurity Alerts. [14] You should document your cyber security policy and use it to train your employees and have as a reference in case of attack. You will want to have it in paper form in case you cannot access your computers. Your policy should outline the procedures for your response. You don't want to be trying to figure out what to do when your office is paralyzed by an attack.

Lawyers are obligated to keep up with technology to protect their clients' interests or to hire someone with the expertise to do it for them. [15] By keeping up with the risks and educating and monitoring you staff, you can avoid having to pay a ransom for your data and the possibility of seeing your clients' data compromised.

Footnotes

a1 ***SHAUN JAMISON is a professor of law with Concord Law School of Kaplan University and is the former chair of the MSBA Practice Management and Marketing Section. Jamison teaches CyberLaw, Legal Research, and the Future of Law Practice. He races in triathlons to stay in shape for online teaching and his social media habit.***

SGJAMISON@GMAIL.COM

1 "Florida Law Firm Hit By Ransomware Scheme." (2/16/2016) *http://www.batblue.com/florida-law-firm-hit-by-ransomware-scheme/*

2 Katie Dvorak, "Hackers return for more money in ransomware attack at Kansas hospital," FierceHealthCare (5/23/2016) *http://www.fiercehealthcare.com/it/hackers-retum-for-more-money-ransomware-attack-at-kansas-hearthospital*

3 "When hackers cripple data, police departments pay ransom," Boston Globe (4/6/2015) *https://www.bo$tonglobe.com/business/2015/04/06/tewksbury-police-pay-bitcomransom-fackers/PkcEIGBTOfU52p31F9FM5L/story.html*

4 Paul, "FBI's Advice on Ransomware? Just Pay The Ransom," Security Ledger (10/10/2015) *https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/,* but see a more recent declaration from FBI Cyber Division Assistant Director James Trainor saying companies should not pay ransom: Katie Dvorak, "Hackers return for more money in ransomware attack at Kansas hospital," FierceHealthCare (5/23/2016) *http://www.fierceheaithcare.com/it/hackers-retum-for-more-moneyransomware-attack-at-kamas-heart-hospital*

5 ABA Model Rule 1.6(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.

6 ABA Model Rule 1.15 - ... property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.

7 Scott Petry, "Law Firms Kill Web Access In The Name Of Cybersecurity," (5/26/2016) Above the Law *http://abovethelaw.com/?sponsored_content=it-Security-vsusers&rf=1*

8 Tara Seals, "Employees Would Sell Passwords for $1000 or Less," retrieved 4/15/2016: *http://www.securion.io/#!Employees-Would-Sell-Passwords-for-1000-or-Less/c14jh/56f137af0cf266a292560bfe*

9 Peter S. Vogel, "Bad news for PE Chang -Court rules that all claims for 2014 data breach are not covered under its cyberinsurance!" Lexology (6/2/2016) *http://www.lexology.com/library/detailaspx?g=4dc04202-1357-4b3c-8c96-43aeac63e00f*

10 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

11 Katie Dvorak, "Poll: Most hospitals have been targets of ransomware attacks," FierceHealthIT, retrieved 4/12/2016: *http://www.fiercehealthit.com/story/poll-most-hospitats-havebeen-targets-ransomware-atutcks/2016-04-11*

12 Mike Mosedale, "Ransomware scam targets lawyers with phony ethics complaints," Minnesota Lawyer (6/7/2016) *http://minnlawyer.com/2016/06/07/yikes-ransornware-scam-targets-lawyers-with-phony-ethics-complaints/*

13 ABA Cyber Security Legal Taskforce *http://www.americanbar.org/groups/leadership/office_of_the_pTesuient/cybersecurity.html*

14 Log in to sign up to receive alerts at this link: *https://shop.americanbar.org/eBus/MyABA/MyLists.aspx*

15 ABA Model Rule 1.1 - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

End of Document

32-FALL Del. Law. 30

Delaware Lawyer
Fall, 2014

Feature

THE DATA SECURITY IMPERATIVE FOR LAWYERS

Edward J. McAndrew

With lawyers top targets for cyberattacks and both firm and client data subject to loss or breach, smart security protocols are essential.

A small law firm is victimized by ransomware encrypting all data on its network. An international law firm is targeted for cyber espionage by a foreign intelligence service. A law firm's network administrator reads attorney emails to obtain material, non-public information that he then uses for stock transactions. A departing employee downloads highly confidential and proprietary data onto USB drives and uploads it to cloud accounts. Hacktivists breach the network of an investigative firm and upload the firm's emails with lawyers on sensitive projects to a public website. A lawyer loses a smart phone containing unencrypted emails and text messages with a client.

These are just some of the types of data security and privacy threats that lawyers now face.

Overview of the Threat Landscape

Data security and privacy have become watchwords of the early 21st Century - for good reason. Digital devices, networks and services collect the details of virtually every aspect of our personal and professional lives. As the Supreme Court recently noted, the search of a mobile phone "would typically expose ... far more information than the most exhaustive search of a house." [1]

The warp-speed adaptation of digital technology has created great challenges to data security and digital privacy. The U.S. intelligence and law enforcement communities have ranked cybercrime as our top national security threat - higher than terrorism or espionage. [2] There is a daily stream of news about hacking: cyber espionage, digital theft of consumer data, money and intellectual property, lost devices exposing private information, and disruption or destruction of digital infrastructure. Nearly half of the adult U.S. population was hacked in the past 12 months. [3]

***31** Cisco's 2014 Annual Security Report aptly stated: "Odds are high that targeted attacks have already infiltrated your networks." [4] Cisco's security software alone blocks 4.5 billion malicious emails and 50,000 network intrusions each day. Most data breaches are never publicly disclosed.

Lawyers and legal services organizations have become significant targets for cyberattacks. Since at least 2009, the FBI has repeatedly issued warnings that hackers are targeting law firms to steal confidential information. In early 2013, a prominent cybersecurity firm estimated that 80 of the 100 largest U.S. law firms suffered data breaches in 2011 alone. [5]

This should not be surprising. Lawyers and legal services organizations are significant aggregators of sensitive data - about themselves, their clients, and their adversaries or counterparts. Like everyone else, lawyers use digital devices

to create, transmit and possess data about their own professional and personal activities, and those with whom they come into contact. Legal services organizations interconnect digitally with clients for practice purposes and with vendors for various purposes - including IT services, building operations (HVAC, security, etc.), client account management, procurement, financial services and human resources.

At risk is the data about lawyers and their organizations, as well as access points to their networks through their clients and business partners. Also at risk is the sensitive, often confidential, client-related data contained in the devices and networks of lawyers and those who assist them. Lawyers also receive sensitive and confidential information from non-clients during litigation transactions, and other matters.

This is not just a problem for large organizations. Symantec reported that 31 percent of the cyberattacks it tracked targeted small and medium-sized businesses with fewer than 250 employees, while 50% of all attacks were aimed at businesses with less than 2,500 employees. Nor is every incident malicious. Nearly 30 percent of the data breaches examined by Symantec involved the accidental loss of digital devices resulting in the exposure of sensitive data.

External cyber actors are far from the only concern. As Edward Snowden has so aptly demonstrated, insiders can simply copy and carry data out of facilities. Users accidentally lose devices containing sensitive data on a daily basis. Even where outside hackers are involved, an authorized user often unintentionally provides them with network access by clicking on hyperlinks or attachments in spear-phishing emails and text messages or by visiting legitimate, but malware-infected, websites.

Ethical Obligations Concerning Client Data Security and Privacy

In August 2012, the American Bar Association issued a report and resolution urging lawyers to use best practices to protect client data from internal and external threat actors. It also amended the Model Rules of Professional Conduct to address technological issues in the practice of law. In January 2013, the Supreme Court of Delaware amended the Delaware Lawyer's Rules of Professional Conduct to track some of the ABA's changes to the Model Rules. Pertinent changes include those listed below.

Rule 1.1 - Competence - Part of a lawyer's duty' to provide "competent representation" requires "keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." [6]

Rule 1.6(c) - Confidentiality - This new subsection requires lawyers to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." [7]

Comment 19 explains that an inadvertent or unauthorized disclosure of confidential information "does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure." [8] The comment lists various factors relevant to this 'reasonableness' determination, "including, but [ ] not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)." [9]

Regarding client-related, electronic communications, Comment 20 states that "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." [10] A lawyer need not employ "special security measures if the method of communication affords a reasonable expectation of privacy." [11] The sensitivity of the information and the extent to which "the privacy of the communication is protected by law or by a confidentiality' agreement" are relevant factors. [12]

Rules 5.1 & 5.3 - Supervision - A lawyer must make "reasonable efforts" to ensure that lawyers and non-lawyers working under the lawyer's supervision, management or control comply with all ethical rules. [13] Comment 3 specifically references outside services, which may include investigative and paraprofessional services, document and data management vendors, and cloud services providers. Factors relevant to the reasonableness of a lawyer's efforts include "the education, experience and reputation of the non-lawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality." [14]

Comment 19 to Rule 1.6(c) also extends a lawyer's data security duty to supervising "other persons who are participating in the representation of the client." [15]

Other rules relating to communication with clients (Rule 1.4) and duties to prospective and former clients (Rules 1.9 and 1.18) also are implicated in the data security' and privacy context. Rule 1.4's duty to "keep the client reasonably informed" and to "promptly comply with reasonable requests for information" may encompass the lawyer's data ***32** security policies and practices. It also may require a lawyer to inform clients *of* cyber incidents impacting the attorney-client relationship. [16] Rules 1.9 and 1.18 may require a lawyer to maintain the privacy and security of data relating to former or prospective clients. [17]

Data Security Leading Practices

Based on the evolving cyber threat landscape and the ethical duties summarized above, each lawyer must be actively involved in data security efforts on an ongoing basis. [18] Although cybersecurity is a relatively new responsibility for lawyers, it does not need to be an overwhelming one. Each lawyer is simply expected to act reasonably under the circumstances in an effort to protect the privacy and security of client data.

The Commission on Law and Technology recently published "Leading Practices: Data Security" on its website to assist lawyers in meeting this obligation. [19] The Leading Practices are drawn from a variety of sources that have been widely adopted across public and private sectors. They therefore may have the added benefit of already having been adopted by some clients, with (hopefully) many more to follow as data security' and privacy practices take root across broader segments of society.

There is no single, correct way to mitigate cyber risk. Nor is there a single checklist to be mechanically applied to each legal practice. The Leading Practices offer suggestions that can be adapted to fit any individual practitioner or organization. Not every Leading Practice will apply to every lawyer. What makes sense for the largest firms with IT departments may not be necessary, or even appropriate, for the solo practitioner or small firm lawyer. There is, however, a general approach to data security that can be used by all lawyers. That general approach and some basic cybersecurity concepts are discussed below. For a more comprehensive discussion, please visit the Commission's website at http://courts.delaware.gov/declt/datasecurity.stm.

Core Concepts and the Basics

Like the cyber threats we face, the task of data security is continuous and dynamic. Below are some basic steps to data security: [20]

- Identify the data, systems and devices to be secured and the threats to them.
- Determine how those threats could impact the lawyer, the organization, clients and others.

- Use the foregoing information to develop a data security plan that fits each lawyer's (or organization's) risk profile, goals, budget, legal and ethical obligations. Educate and train all users on the plan.
- Implement and monitor the effectiveness of the data security plan.
- Create a cyber incident response plan for data breaches and other cyber incidents (system crashes, destruction of data, etc.) that might impact a practice. Educate and train all incident responders on the plan.
- Adjust both plans as variables change.

Cyber incidents cannot be entirely eliminated. Many of them can be mitigated, though, by employing basic cyber hygiene and security measures. Summarized below are some of these measures, categorized by how lawyers most commonly create, store and transmit sensitive data.

Devices and Networks

Secure computers, mobile phones, tablets, USB and other portable drives, digital media and all devices that connect to the network with strong passwords and encryption. Prohibit the sharing of devices. Require that any USB drive or other portable media be encrypted before they may be used. Continually update and patch software and browser vulnerabilities. Employ capabilities to remotely lock, locate and erase data from any mobile device that connects to the network.

Avoid using public Wi-Fi networks to access confidential and sensitive client information. Instead use private, encrypted hotspots or virtual private networks to access such information. Require multifactor authentication to access networks and online accounts. Limit remote access privileges to essential users.

There are many additional considerations for networks. Listed here are just a few that should be used for even basic networks. Allow only known users and devices with approved configurations to access a network, and monitor that access/use. Utilize and continually update firewalls and anti-virus, anti-spam, anti-spyware, malware and phishing defenses for networks. Protect confidential and sensitive data with appropriate encryption technology. Restrict access to sensitive information or network areas on a "need-to-know" basis. Tightly control the use of network administrative and other broad-access privileges. Engage in the continuous monitoring of IT systems, networks, security status and risks. Disable any unnecessary or unused accounts. Monitor and control remote access from all endpoints, including mobile devices.

Electronic Communications (Email, Text, Instant and Voice Messaging)

Encrypt communications that contain confidential client information. Transmit decryption keys/passwords via separate communication. Do not transmit confidential client information to personal accounts. Consider transmitting highly sensitive client information through a secure file transfer protocol (FTP) or file sharing service. Do not access confidential client information from shared or untrustworthy devices.

Cloud Services Security

Establish a policy on whether and which cloud services may be used and what data may be stored in those services. Many file hosting programs and applications, such as Dropbox and Sky-Drive, are public repositories of data. Confidential and sensitive client information generally should not be stored in such public repositories without strong encryption. Ensure that cloud providers: (1) have no ownership or security interest in data stored in the cloud; and (2) have an enforceable

obligation and have taken reasonable steps to secure that data. Be able to obtain all stored data on demand. Know where the data is physically being stored, and comply with all applicable security and privacy laws.

Data Retention, Recovery and Destruction

Perform complete and frequent backups of critical systems, data and devices, with appropriate encryption employed. Have a backup plan in case data stored in a cloud becomes inaccessible. Employ ***33** remote wiping or deletion capability for lost mobile devices, laptops, tablets and other portable digital media. Develop data retention and destruction plans that include protocols for the removal and destruction of all confidential and sensitive data prior to disposal of all devices. Keep only that data that is needed or is required to be kept.

The Way Forward

Taking reasonable steps to protect client information is nothing new. Confidentiality has always been the keystone of the attorney-client relationship, and we have been using digital technology to practice law for decades. What has changed is the threat landscape, and it will continue to do so.

Cyber threats, and the magnified and deleterious consequences they can bring, require each of us to incorporate digital data security into our practices. We need to educate ourselves and each other about these new threats and develop plans for addressing them. The data security imperative now arises daily, can be daunting, but is doable.

Footnotes

1 *Riley v. California,* 134 S. Ct. 2473, 2491 (2014).

2 Director of National Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community" (Jan. 29, 2014) (prepared statement before Senate Select Committee on Intelligence), *available at* http:// www.dni.gov/index.php/newsraom/testimonies/203-congressional-testimonies-2014/1005-statcment-for-the-record-worldwide-thrcat-asscssmcm-of-the-us-intelligence-community; Greg Miller, "FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered," WASH. POST (Nov. 14, 2013), *available at* http://www.washingtonpost.com/world/national-security/fbidirector-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11c3--9890-a1c0997fb0c0_story.html=wprss=rss_ world.

3 *See, e.g.,* Jose Pagliery, "Half of American Adults Hacked this Year," *available at:* http://money.cnn.com/2014/05/28/ technology/security/hack-data-breach/.

4 CISCO 2014 Annual Security Report, *available at:* https:// www.cisco.com/web/offers/lp/2014-annual-security-report/ index.html? keycode=000350063.

5 MANDIANT INTELLIGENCE CENTER REPORT, APT 1: EXPOSING ONE OH CHINA'S CYBER ESPIONAGE UNITS 20, *available at:* http:// intelreport.madiant.com/Mandiant_APT1_Report.pdf.

6 DEL. RULES PROF'L CONDUCT R. 1.1 cmt. 8 (2013).

7 *Id.* R. 1.6(c).

8 *Id.* R. 1.6(c) cmt. 19.

9 *Id.*

10 *Id.* R. 1.6(c) cmt. 20.

11 *Id.*

12 *Id.*

13 *Id.* R. 5.1, 5.3 cmts. 3 & 4.

14 *Id.* R. 5.3 cmt. 3.

15 *Id.* R. 1.6(c) cmt. 19 (citing DEL. RULES PROF'L CONDUCT 1.1, 5.1, 5.3).

16 *Id.* R. 1.4(a)(2)-(4).

17 DEL. RULES PROF'L CONDUCT 1.9, 1.18.

18 THE ABA CYBERSECURITY HANDBOOK 4 (2013). This book is an excellent resource that summarizes many of the legal and ethical data security and privacy standards applicable to lawyers. It also provides suggested approaches to data security for lawyers practicing in different settings.

19 Delaware Supreme Court Commission on Law & Technology Website, *available at:* http://courts.delaware.gov/declt/datasecurity.stm.

20 Specific steps to formulating data security and incident response plans, as well as suggested technical components of a data security plan, can be found on the Commission's website, at http:// courts.delaware.gov/declt/datasecurity.stm.

End of Document

300-JUN N.J. Law. 54

New Jersey Lawyer, the Magazine
June, 2016

Professional Malpractice
Feature

GETTING SERIOUS ABOUT LAW FIRM CYBERSECURITY

Karen Painter Randall, Steven A. Kroll [a1]

One can hardly turn on the news these days without hearing about the latest victim of a cyber-attack. Industries across the board, from large retailers to healthcare providers to even the U.S. government, have been the targets of advanced cyber-attacks where millions of personal identifiable information (PII) was stolen. The legal profession is not immune from the threat of a costly cyber incident. In fact, the FBI has issued warnings and held meetings with nearly all of the top law firms in New York about the risk of a data breach and theft of confidential and proprietary client information. Since at least 2009, the FBI, the U.S. Secret Service, and other law enforcement agencies have warned law firms that their computer files were targets for cyber criminals and thieves in China, Russia, and other countries, including the U.S., looking for valuable confidential and proprietary information including corporate mergers, patent and trade secrets, litigation strategy, and more.

Many law firms have, in fact, suffered some sort of data breach. For example, according to recent reports, the computer networks of Cravath Swaine & Moore LLP, Weil Gotshal & Manges LLP and other major law firms were penetrated by unknown hackers possibly looking to profit from confidential or insider information for publicly traded companies. The FBI and federal prosecutors with the Southern District of New York have opened an investigation to determine if any confidential information was stolen by hackers and used for insider trading, according to the *Wall Street Journal,* which cited anonymous sources. Reportedly other prominent firms had their networks breached and hackers were threatening further attacks. Cravath said it suffered a "limited breach" of its computer network last summer, but that the firm was "not aware that any of the information that may have been accessed has been used improperly," according to the *Wall Street Journal.*

The American Bar Association (ABA) described law firms as both "attractive" and "soft" targets for a cyber-attack. Law firms are attractive targets because they handle a variety of high-value information, such as intellectual property, insider information on corporate deals and mergers, as well as the PII and protected health information (PHI) of both clients and other parties involved in a lawsuit. This includes heavily regulated information such as health and financial information. Moreover, law firms are considered soft targets because while ***55** other industries have devoted a significant amount of time and money to ensure that sufficient policies and procedures are implemented to protect against a cyber-attack, law firms often dedicate less resources and simply lack awareness of the latest cybercrime trends.

In light of this, to take a proactive approach to cybersecurity, it is crucial that law firms understand the types of data being targeted by hackers, as well as both the legal and ethical responsibilities owed to their clients. If nothing else, from a business standpoint, many clients are now demanding that their law firms do more to protect their sensitive information to ensure they do not become 'back doors' for hackers.

For example, it has been reported that J.P. Morgan Chase & Co., Morgan Stanley, Bank of America Corp., and UBS AG are just a few of the larger financial institutions that have subjected outside law firms to greater scrutiny regarding

their cybersecurity. This includes law firms completing 20-page questionnaires about their threat detection and network security systems, as well as some sending their own security auditors into firms for interviews and inspections. Thus, this article focuses on this new threat facing law firms, and some basic security steps that can be taken to protect against a costly cyber incident.

Ethical Obligations

Pursuant to the Rules of Professional Conduct, attorneys must take reasonable steps to protect their clients' information. Namely, RPC 1.6(a) requires an attorney not reveal confidential information, and RPC 4.4(b) discusses an attorney's duty to take reasonable steps in communicating with clients, as well as the duty to respect the privilege of others. Additionally, ABA Rule 1.1, Comment 8, makes clear that there is an ethical obligation related to competent representation that requires counsel to stay current on the risks posed by technology and take reasonable action to protect against those risks.

Despite these principles, many attorneys still fail to take the necessary steps to protect their clients' confidential information, even in the context of a small task such as sending and receiving emails. According to the 2015 edition of the annual Legal Technology Survey Report, compiled by the American Bar Association's Legal Technology Resource Center, only 35 percent of lawyers used email encryption. That percentage has remained virtually unchanged over the last four years of the survey, despite recent headlines regarding cyber-attacks on large corporations, such as Anthem, Inc., and the U.S. government.

When the survey asked what security precautions attorneys were implementing when sending confidential and privileged communications to clients via email, the answer given by 71 percent of the attorneys was that they rely on the confidentiality statement in the message body. Additional methods used by attorneys to protect the information and content contained within an email sent to a client included: a confidentiality statement in the subject line, requiring clients provide written or oral consent, password-protecting documents and using registered email. Moreover, of the lawyers who responded that they use encryption, a third could not say what kind of encryption they implemented. Those who could say what type of encryption they used most commonly identified it as general-purpose software with encryption features that required the recipient to be sent a separate password. Thus, it is no wonder that a recent Citigroup internal report warned bank employees that digital security at many law firms remained subpar, and that law firms would continue to be targeted by malicious actors looking to steal confidential information.

Top Cyber Threats Facing Law Firms

Although there are many different forms of cyber threats, the following are a few of the top ones facing law firms today. The first form involves spear-phishing emails, or malicious messages tailored to individuals in order to appear legitimate, which are used to infect a specific target. For example, an attorney may receive an email from a hacker pretending to be a client, requesting that he open an important attachment. If opened, it infects the entire computer network with malware. According to the Justice Department's indictment of five members of the Chinese military in May 2014, spear-phishing emails were used to steal, among other things, privileged attorney-client communication related to SolarWorld's trade litigation with China.

The second form involves ransomware, which encrypts a victim's files and then attempts to sell the victim a key to unlock their data. In many cases, victims of ransomware either pay the extortion or lose access to the critical files if they are not backed up.

In Feb. 2015, the law firm Ziprick & Cramer, located in California, sent out a letter to its clients advising that on or about Jan. 25, 2015, the firm was the victim of a single cyber-attack, by a relatively new variant of a Cryptolocker-type

virus. A Cryptolocker is a kind of ransomware used to encrypt files so they become unreadable, and the hackers then demand money to restore the data. The firm reported it to the FBI and called in a cyber forensic specialist to assess the damage and install safeguards to thwart future attacks. The publicity alone involving this cyber incident surely had an impact on clients' confidence.

The third form involves hacktivist groups such as Anonymous, which target law firms involved in controversial cases. While law firm Puckett & Faraj represented a staff sergeant accused of leading a group of Marines responsible ***56** for the deaths of 24 unarmed Iraqi civilians, it had its email accounts hacked, and more than two gigabytes of correspondence stolen and leaked. The firm's Google email passwords were not secure enough to keep out hackers, who may have employed equipment that can rapidly use multiple possible combinations to break in. Fortunately, the firm characterized the stolen documents as “really innocuous.”

Steps to Increase Cybersecurity

In light of the above, many law firms are now taking steps to increase data security and ensure that proper policies and procedures are in place to protect against a cyber-attack. First and fore-most, preparation is vital to preventing any sort of attack. Thus, law firms should create a cross-organizational committee, which includes not only management but human resources, procurement, finance, internal and external cybersecurity counsel, and information technology (IT) to develop and implement a risk management plan for preventing a data breach. Moreover, many law firms are now using a chief technology or privacy officer to oversee the firm's data security and privacy, as well as technology infrastructure, to ensure the policies and procedures are consistent with the security plan and technology-

Once a committee has been established, policies should be implemented regarding the privacy and security of the firm's data, which includes the use of encryption, remote access, mobile devices, laptops, email accounts, and social networking sites. In addition, a law firm should conduct an inventory of the software systems and data, and assign ownership and categorization of risk. (The higher the sensitivity of the information, the stronger the security protections and access control must be.) Furthermore, the IT department should conduct third-party vulnerability scans, penetration tests, and malware scans to protect against potential data breaches. The use of antivirus software is simply not enough to detect sophisticated attacks, which sometimes go undetected for an average of 300 days.

Most importantly, after setting the tone from the top, law firms must train employees so they are aware of the company's security protocol and are protected against the potential for accidentally exposing a client's personal, confidential information with the click of a button. This also includes having all employees create strong and unique passwords to protect their computers and mobile devices in conjunction with a password management utility. In addition to implementing the use of secure account credentials, other commonly deployed methods and tools used to keep data safe include encryption, as well as physical securities.

Clearly, the use of encryption for emails is a must-have tool for attorneys. Encryption apps, such as Virtru, are very easy to use and protect clients' data and privacy when sending sensitive emails and attachments. Also, some law firms are instructing attorneys not to open attachments sent via email unless they are in a secure environment in the office, or using a firm laptop on an encrypted line. For particularly sensitive matters, some law firms are going so far as restricting work to stand-alone computers that do not connect to the Internet. Additionally, as discussed already, mobile devices are a particular focus, as many firms can wipe data from smartphones and laptops that are lost or stolen, as well as install some level of encryption.

Unfortunately, in the evolving technological world even the best security can be penetrated by skilled hackers from around the world. Thus, besides having policies and procedures in place to prevent a data breach, it is critical that a law firm be prepared to act quickly in the event a breach is detected. The cybersecurity committee must constantly collaborate to implement and test a rapid response plan to react to a cyber incident quarterly. The plan should identify rapid response

team members from each office the firm operates, along with the contact information for key law enforcement, public relations and cyber forensic experts.

Once a potential data breach has been identified, a law firm should work with its cyber forensic experts to act quickly to identify what type of information was exposed and remediate while preserving the attorney-client privilege. It should be noted that each state has its own notification laws relevant to reporting a data breach; thus, the response team should be familiar with the notification requirements. For example, in New Jersey the statute is triggered upon discovery or notification of a breach of security. 'Breach of security' means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. [1] If the law firm that suffered a data breach affects a national client, the notification process may become even more complicated, since there are currently 47 states that have notification laws, which vary in scope.

Cybersecurity Liability

Aside from a claim for attorney malpractice, various state and federal regulatory agencies have taken the forefront in prosecuting claims against businesses that fail to have proper policies and procedures in place. For example, should general PHI be stolen this would implicate the Health Information Technology for Economic and Clinical Health Act ***57** (HITECH). The law was enacted in 2009 as part of an overall effort to modernize medical record keeping and PHI, and update parts of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In particular, HITECH expressly requires HIPAA "covered entities" to report PHI data breaches affecting 500 or more individuals to the affected class, the Department of Health and Human Services (HHS) and the media within 60 days of an event. [2]

Although one may question how this requirement applies to law firms, as defined under HITECH, 'business associates' expressly include entities providing legal services to HIPAA-covered entities. Thus, there is no question that a law firm is a HITECH business associate, and, as such, responsible under the law to secure PHI, provide appropriate notification, and otherwise comply with HIPAA standards. Furthermore, HHS's Office for Civil Rights (OCR) enforces compliance with PHI data regulations. To demonstrate the potential for damages, on May 7, 2014, OCR issued a press release announcing that two healthcare organizations--New York and Presbyterian Hospital and Columbia University-- agreed to resolve charges that they potentially violated HIPAA by failing to secure thousands of patients' electronic protected health information (ePHI) on their network. The monetary payments totaled $4.8 million, which is the largest HIPAA settlement to date.

In addition to HHS-OCR, another regulatory body enforcing cybersecurity compliance is the Federal Trade Commission (FTC). On Aug. 24, 2015, the Third Circuit affirmed the District Court of New Jersey's ruling confirming the FTC's authority to investigate and prosecute consumers' privacy by failing to maintain appropriate data security standards. [3] While there have been no instances reported, to date, where the FTC has prosecuted a law firm for cybersecurity issues, a law firm should be prepared to face scrutiny from the FTC, as the number and scope of enforcement actions involving cybersecurity continues to increase.

Sharing Data with Other Law Firms

It is also important that law firms keep abreast of the ever-changing landscape of cybersecurity and what types of threats and vulnerabilities are out there. Along those lines, in Aug. 2015, the Legal Service Information Sharing and Analysis Organization (LS-ISAO) was launched. It alerts law firms to potential cyber threats and vulnerabilities. The Financial Services Information Sharing and Analysis Center, also known as FS-ISAC, the financial industry's forum for cyber threat discussion, is providing guidance and support to the LS-ISAO.

Although law firms normally receive their information regarding a potential cyber threat from other sources, such as trade groups, the LS-ISAO provides them with a centralized platform to share information anonymously. This service is consistent with an executive order issued by President Barack Obama this past year, which encourages the development of platforms where cybersecurity information can be shared within the private sector, as well as with the government.

In order to become a member of LS-ISAO, a law firm must submit an application, pay a fee, and meet certain eligibility criteria. Once enrolled, law firm members will receive email alerts and advisories on cyber threats and vulnerabilities, as well as physical threats. Moreover, law firms will be able to submit their own information anonymously regarding a cyber incident.

Although there are some who believe this new information-sharing forum will not significantly benefit law firms in preventing a cyber-attack, many believe the creation of the LS-ISAO is a step in the right direction for law firms to become more proactive in protecting against a potential cyber breach. Ultimately, the goal of LS-ISAO is to share information about these potential cyber-attacks and help law firms mitigate their damages.

Damages

According to a 2015 study conducted by the Ponemon Institute, the average cost of a data breach is $6.5 million, or $217 per lost or stolen record. This includes first-party losses such as retaining a forensic IT investigation firm, network remediation, data recovery and restoration, implementation of new safeguards, and the cost of business interruption. Moreover, should a law firm become involved in a civil lawsuit, or the target of a regulatory enforcement action, this would constitute third-party losses such as paying legal defense costs, credit monitoring services, and any other connected damages or fines. Besides the obvious financial cost of a cyber-attack, a law firm would also have to deal with damage to its reputation; in particular, seeking to regain the trust of clients who entrusted the firm with their confidential information.

As a result, lawyers and law firms that do not want to face cyber liability and wish to transfer some of the risk to other sources should consider cyber liability insurance. Besides being covered for first- and third-party losses, often the insurer will get involved at the early stages to appropriately guide its policyholder and retain counsel, public relations firms, IT consultants, and similarly experienced professionals, while actively managing the risk and cost. Thus, a law firm should consider reviewing its current insurance policies to see what is and is not covered, and then meet with an insurance broker well versed in cyber coverage about procuring insurance. When the average cost of a cyber-attack is $6.5 million, cyber insurance appears to be worth the expense.

*58 Conclusion

In a profession based upon tradition and precedent, the practice of law must keep pace with the changes in technology in order to continue to preserve the legal and ethical duties owed to clients. Unfortunately, most cyber experts say it is not a matter of if, but when. Thus, law firms must be prepared for a cyber incident or face the costly ramifications of a cyber-attack involving clients, regulators and law enforcement. With so much at stake, at the very least law firms should have a basic understanding of the cyber risks facing them today, so they can manage risk and compliance relevant to PHI, PII and privacy issues. Under best practices it is critical that cyber liability insurance and a reasonable security program are put in place to protect clients' data, and that a rapid response and business continuity plan be prepared and rehearsed periodically to protect the firm and mitigate damage.

Footnotes

a1 ***Karen Painter Randall,*** *a certified civil trial attorney and complex litigation partner with Connell Foley LLP in Roseland, is co-chair of the firm's cyber security and data privacy and professional liability groups. A member of the International Association of Privacy Professionals, she counsels clients, including law firms, on the data protection and regulatory compliance laws tailored to the enterprise and develops proactive plans to reduce the risk of a cyber-attack.* ***Steven A. Kroll*** *is an associate with Connell Foley LLP in Roseland. In addition to representing professionals in various areas, he concentrates his practice in the areas of professional liability, cyber liability, general insurance litigation and employment law handling matters in both New Jersey and New York.*

1 N.J.S.A. 56:8-163-66.

2 42 U.S.C. § 17932.

3 *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

End of Document

How to Prepare to Defend Your Law Firm's Reputation in the Event of a Cyber-Attack

tmgroup

Global, USA | November 21 2016

With cyber-crime making the headlines more and more frequently, it is becoming increasingly important that law firms of all sizes understand how to handle such a situation professionally and keep their reputation intact.

Here are some steps any law firm can take to help ensure that a cyber-attack or data breach doesn't cost them their client base.

The focus must be on fixing the problem and retaining your clients trust

The key to surviving a cyber-attack with your reputation intact is in what you do beforehand – in planning, thinking, training and rehearsal – as delivering a slow, haphazard, confused, overly legalistic or contradictory response will only exacerbate the situation.

Your plan needs to focus on 2 key areas: 1. Fixing the problem as quickly as possible 2. Retaining the trust of stakeholders and clients whose information may have been compromised

Discuss what "worst case scenario" means to your firm

When creating your plan, a good starting point is to sit down with your senior team and conduct a cyber reputational risk analysis, in essence decide what your "worst case scenario" looks like.

Every law firm will have a different view on what defines a "worst case scenario". You need to understand what this scenario is to be able to recognise when it is happening – and (just as importantly) when it isn't happening.

This will help everyone to understand the magnitude of a situation, should something arise, and respond accordingly.

Create a cyber incident response plan for these different situations

In a high pressured situation, you don't want to be making snap judgements, as this could lead to mistakes which could be difficult to recover from.

Set aside time to work through some of your "worst case scenarios", and discuss what decisions will need to be made and who will be responsible for making them.

You should also make a list of the different phone numbers you will need. This list should include nominated individuals who will "take the helm" of the situation, as well as the people whose advice, support and technical services you will require to get your operation back up and running.

Having all of this information readily available will help ensure you are contacting the right people as quickly as possible, removing any unnecessary stress and delay.

Decide how and when you are going to communicate with those affected

Don't make the mistake of thinking you can hide your breach from your clients; they have a right to know that their data has been compromised. It is also far better your clients hear the news directly from your firm, then to find out through a third party, rumour or through the media.

When communicating the news to your clients, it is best to adopt a personal approach. For example, if only a small number of clients have been affected, it is in your firm's interests for a senior individual to phone them.

However, if hundreds of clients have been affected, you will need to adopt a speedier and more realistic approach. For example, sending out an email explaining what has happened and what your clients need to do next.

As part of your planning process, it can help to put together an email template which can be quickly edited and sent out in the event of a cyber-attack. You should also write some guidelines on how quickly you will be prepared to talk to your clients, looking at possible triggers, and the pros and cons of sending out various communications.

Have a back-up communication plan for if your systems are still compromised

You also need to think about how you would communicate if your systems were still compromised.

For example, if you can't send out an email or display a message on your website because your systems have been taken down.

In such a situation, could you relay the message via phone or Facebook?

Be prepared for the media to get in touch

Once you have communicated the news to your clients, you need to be prepared for the media to get in touch. Remember, emails can be forwarded!

It is wise to nominate 2-3 individuals in advance who are prepared to step forward; to avoid your one point of contact being on holiday if a situation occurs.

It is equally important that your nominees have media training, as they may have to answer questions when they only have access to limited information, but will still need to reassure everyone and communicate effectively.

Brief your colleagues before going public

Before you communicate any news to your clients, you need to make sure you have briefed your internal staff first. (You can put a template briefing document together as part of your planning.)

This will help to ensure that anyone in meetings or taking phone calls is knowledgeable of the developing situation, and is responding consistently in line with the organisation's key messages.

Your clients won't expect you to be invincible – but they will expect a professional response

No one is immune to the threat of a cyber-attack, and as time goes on it will become almost inevitable that every law firm will experience some kind of data breach.

While it is unreasonable for a stakeholder or client to expect an organisation to be invincible, they will expect your law firm to demonstrate a well-considered and speedy response to correct the situation.

With thanks to Jonathan Hemus from Insignia (http://insigniacomms.com/), Crisis management, training, planning & consultancy