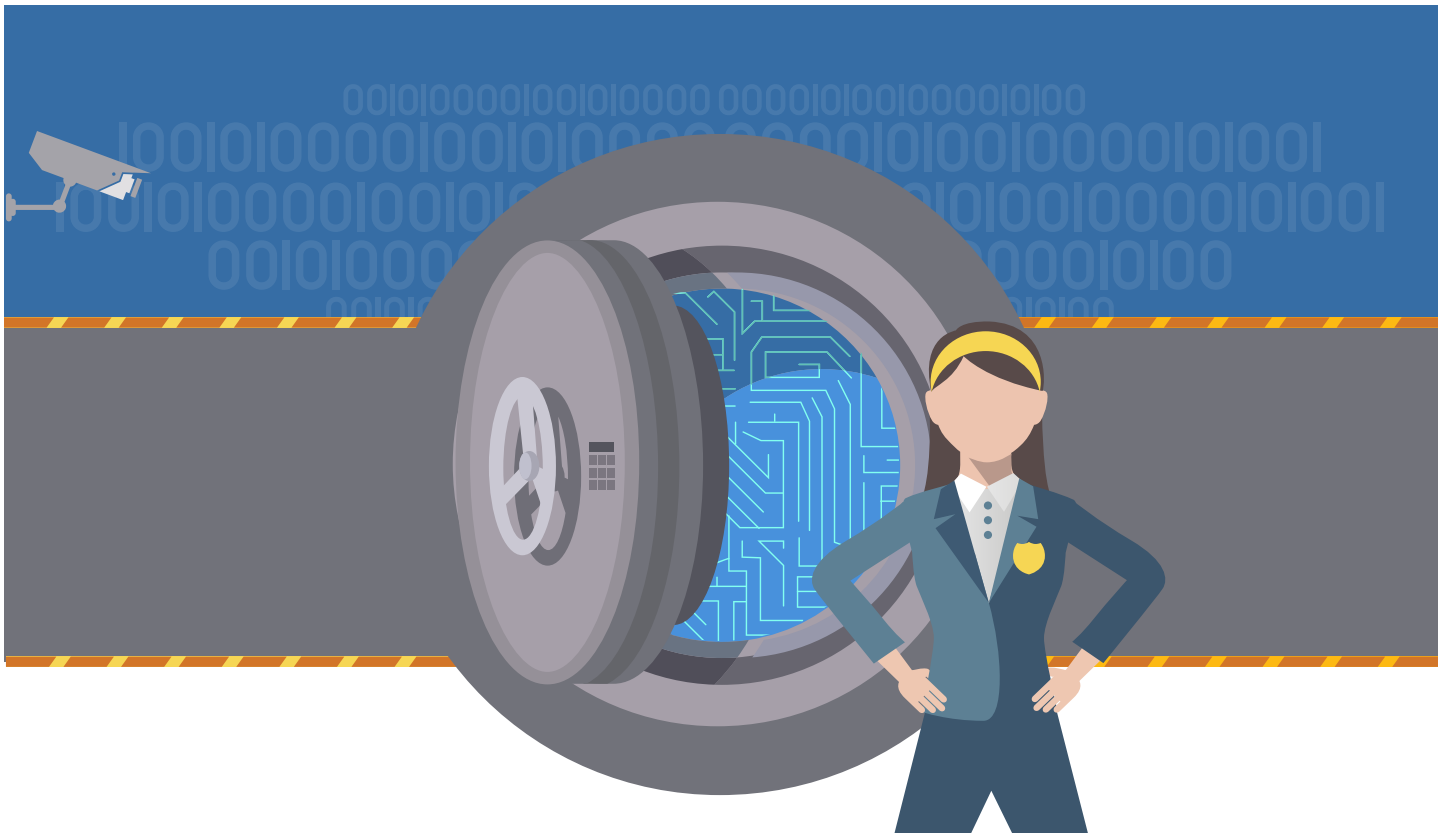
12 Steps to Cybersecurity: A Guide for Law Firms

Brian Focht



12 Steps to Cybersecurity

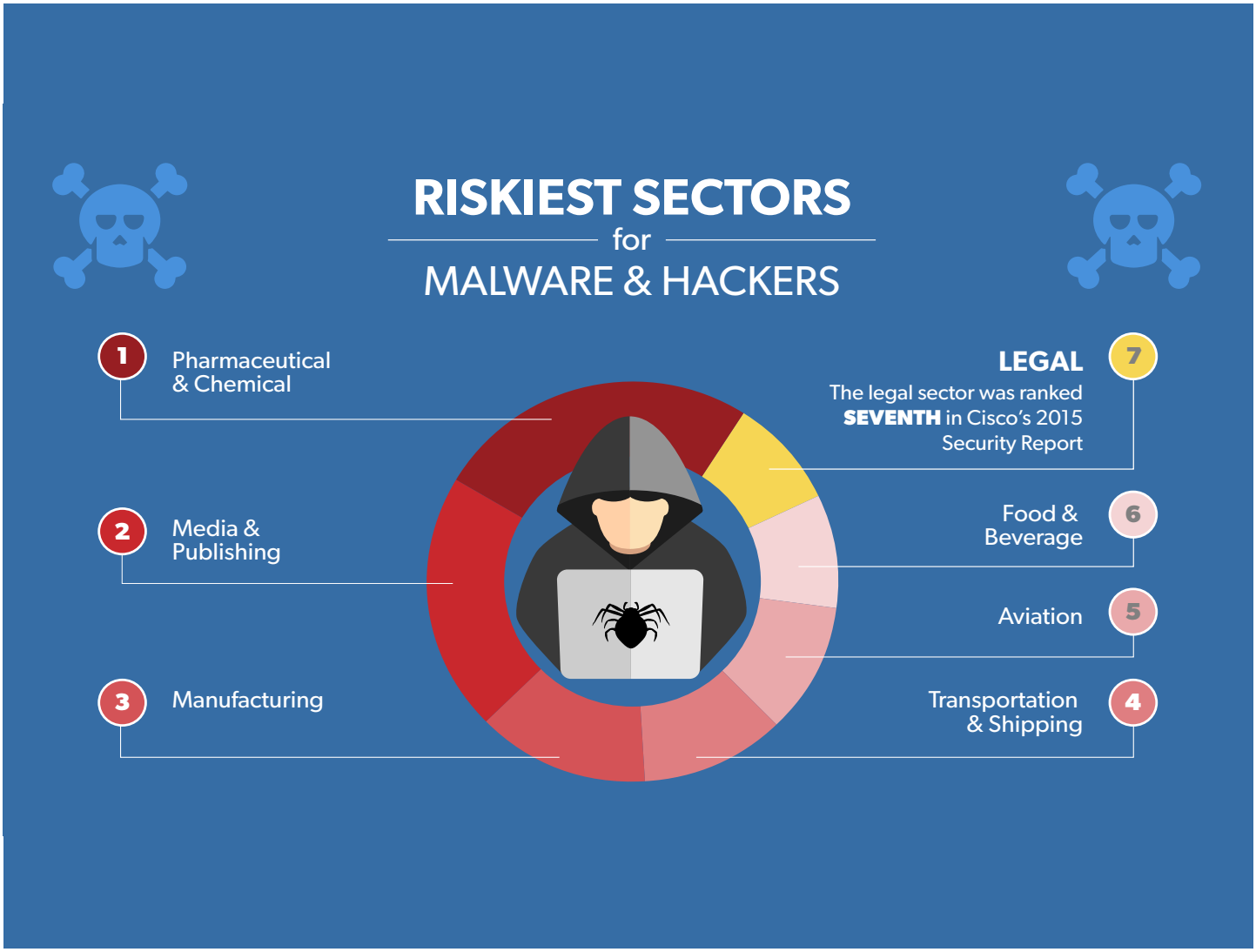
Whether you admit it or not, your law firm is vulnerable. While 79% of respondents in a 2014 law firm cybersecurity survey ranked cybersecurity as one of their top 10 risks, fewer than 28% had actually assessed the cost of a data breach.[1] Your files contain valuable confidential information[2]—confidential client information, birthdates, credit card numbers, Social Security numbers, all nicely organized and easy to access.

Hackers are wising up to the wealth of data available from most law firms.[3] They know how to find that valuable information and how to get it. They also know that most law firms don't appreciate the threat that cyber attacks present, and are vulnerable. In fact, Cisco ranked legal as the seventh most vulnerable industry in their annual security report.

A successful cyber attack exposes you to financial liability,[4] can ruin your reputation,[5] and put your law license in jeopardy. It's a modern day fact of life: you're vulnerable—but exactly how vulnerable is up to you.

You can never completely eliminate the risk posed by cybersecurity threats, but by implementing a cybersecurity policy, you can significantly reduce it.[6] However, it can't be just any policy. The *right* cybersecurity policy isn't one-size-fits-all, but rather one that is designed to accommodate your law firm's unique character and circumstances.

Creating such a policy isn't easy without help. That's why we've developed a comprehensive 12 Step Checklist in conjunction with Brian Focht, The Cyber Advocate, for creating the right cybersecurity policy for your law firm.



1 More Cyber Preparedness Needed, According to 2014 Law Firm Cyber Survey, MARSH USA (Jan. 15, 2015), http://usa.marsh.com/NewsInsights/ThoughtLeadership/Articles/ID/43529/More-Cyber-Preparedness-Needed-According-to-2014-Law-Firm-Cyber-Survey.aspx.

2 Joseph M. Burton, 4 Steps to Getting Serious About Law Firm Cybersecurity, LAW PRAC. TODAY (Sept. 15, 2014) http://www.lawpracticetoday.org/article/4-steps-getting-serious-law-firm-cybersecurity/.

3 Lolita C. Baldour, FBI: Hackers targeting law and PR firms, ASSOC. PRESS (Nov. 17, 2009, 10:58 AM), available at http://www.nbcnews.com/id/33991440/ns/technology_and_science-security/t/fbi-hackers-targeting-law-pr-firms/#.VSauxvAYHCU.

4 IT Security Risks Survey 2014: A Business Approach To Managing Data Security Threats, KASPERSKY LAB, 18-20, http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf (last visited on April 5, 2015) [hereinafter Kaspersky 2014 Survey]; Alex Williams, Target May Be Liable For Up To $3.6 Billion From Credit Card Data Breach, TECH CRUNCH (Dec. 23, 2013), http://techcrunch.com/2013/12/23/target-may-be-liable-for-up-to-3-6-billion-from-credit-card-data-breach/.

5 Kaspersky 2014 Survey, supra note 4, at 21.

6 Ari Bai and Nick Verderame, Cyber Attacks are a Risk for Businesses of All Sizes, LAW TECH. TODAY (March 27, 2015), http://www.lawtechnologytoday.org/2015/03/cyber-attacks/.

Step 1: Identify Your IT Manager

Identifying and empowering an IT manager is critical to the success of your cybersecurity policy. Your IT manager needs to be an expert—not an unpaid intern. Whether internal or a third-party contractor,[7] this person must be an experienced and knowledgeable IT professional.

Your IT manager also needs oversight.[9] Determine specifically where the role fits within your organization. Your IT manager runs your cybersecurity based on your direction and policies,[10] not their own whims, preferences, or personal beliefs. Oversight cannot be nominal—rather, it must be active and respected. The supervision is not there because you want to dictate to your IT manager, or because of a lack of trust. The supervision is there because it's necessary.

(The option for an internal IT professional is a more likely option for medium and large law firms. Solo and small firms will need to rely on third-party vendors or outsourced IT.[8] Fortunately, the role of IT manager is not a full time position in most small firms.)

7 2014 Legal Technology Industry Survey: The Emergence Of Tigers And Bears And Other Law Firm Trends, ADERANT, available at http://pages.aderant.com/WC2014-14Tigersvs.BearsReport.html (last visited April 5, 2015).

8 Id. at 6.

9 cybersecurity and the Duty of Care, DLA PIPER (Feb. 9, 2015), http://www.slideshare.net/DLAPiper.

10 Jim Calloway, IT Governance: A Critical Issue for Law Firms, A.B.A., available at http://www.americanbar.org/publications/law_practice_magazine/2014/july-august/practice-management-advice.html (last viewed April 5, 2015).

Your IT manager will have several responsibilities, including:

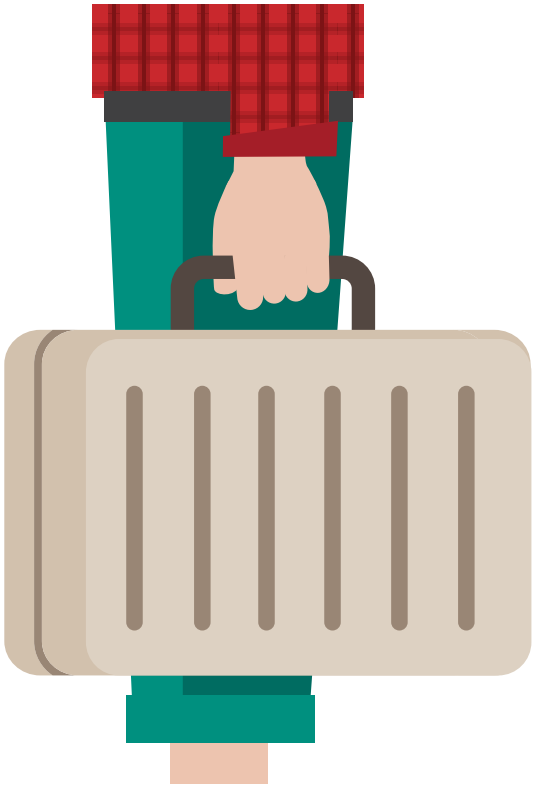
1. **Enforce your cybersecurity policy** – Implement, administer and enforce your cybersecurity policy.
2. **Conduct regularly scheduled Cybersecurity audits** – Ensure compliance with your cybersecurity policy and test its effectiveness.
3. **Install and maintain security software** – Research and recommend security and anti-virus systems (including email and web filters); install and update the systems your law firm uses.
4. **Establish and implement a system for operating system and software updates** – Whether through regularly scheduled updates or through automation, ensure that all operating system and software updates are installed, especially critical security updates.
5. **Application Whitelisting**[11] *(Optional)* – Reduce your potential vulnerability to cyber attacks by limiting software and apps your employees are allowed to use to those designated by your IT manager. Bear in mind, though, that Whitelisting isn't without costs and trade-offs:
   - Attorneys and staff may find Whitelisting to be restrictive;
   - May delay use of new programs and apps; and
   - A poorly implemented Whitelisting program may reduce morale and compliance.

   In my opinion, if you use Whitelisting, only use it for major types of programs and applications, such as cloud storage, law practice management systems, and file transfer programs.

Make sure it fits your law firm:

Your IT manager is a part of your law firm. They must be able to work with your attorneys, and staff. The prototypical cranky IT guy who gets annoyed by the complaints of other company employees need not apply. Your IT manager is a part of your team—any conflicts will prevent your IT manager from being effective.

11 Small Firms Cybersecurity Guidance: How Small Firms Can Better Protect Their Business, SIFMA, 6-7, available at http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/.



Step 2: Create a Data Classification Framework

This is a fancy way of saying 'organize your data based on how valuable it is.' There are two parts to your framework: 1) General Classification and 2) Confidential Classification. Your cybersecurity policy is going to depend a lot on knowing what you're keeping safe.

1 General Classification

The first part involves categorizing all of your data into one of three categories:[12]

General Use Data: information that is generally available or made available to the public, such as information published on your law firm website and included in public releases or disclosures.

Internal Use Data: non-confidential information that is unavailable to the public without prior authorization, such as internal communications. This category includes information that, if released publicly, may cause embarrassment, but would otherwise only cause minimal harm.

Confidential Data: information that you have a legal obligation to keep private.

2 Confidential Classification

The second part involves information you've classified as Confidential Data. Create sub-categories within the Confidential Data category based on the nature of your legal obligation to protect the data. For example, I group my data as follows:

- Information subject to protection under specific government statutes or regulations, such as medical records protected under HIPPA[13] or financial information protected by the IRS[14];
- Commercially sensitive information, such as trade secrets, future business plans, or negotiation strategies;
- Information you are contractually obligated to protect, such as information subject to your cyber insurance policy or a particular client agreement; and
- Confidential information not subject to any specific protection system outlined above.

Tip

You may also want to determine whether access to certain information will be restricted. If you do, make sure that the restrictions are appropriate, that the right people have access, and that they understand the importance of keeping login credentials secret.

Make sure it fits your law firm:

Creating a data classification framework is crucial for ensuring that your cybersecurity policy is right for your firm. An effective response to a cyber attack may not be the same for different information (i.e. intellectual property vs. medical records).

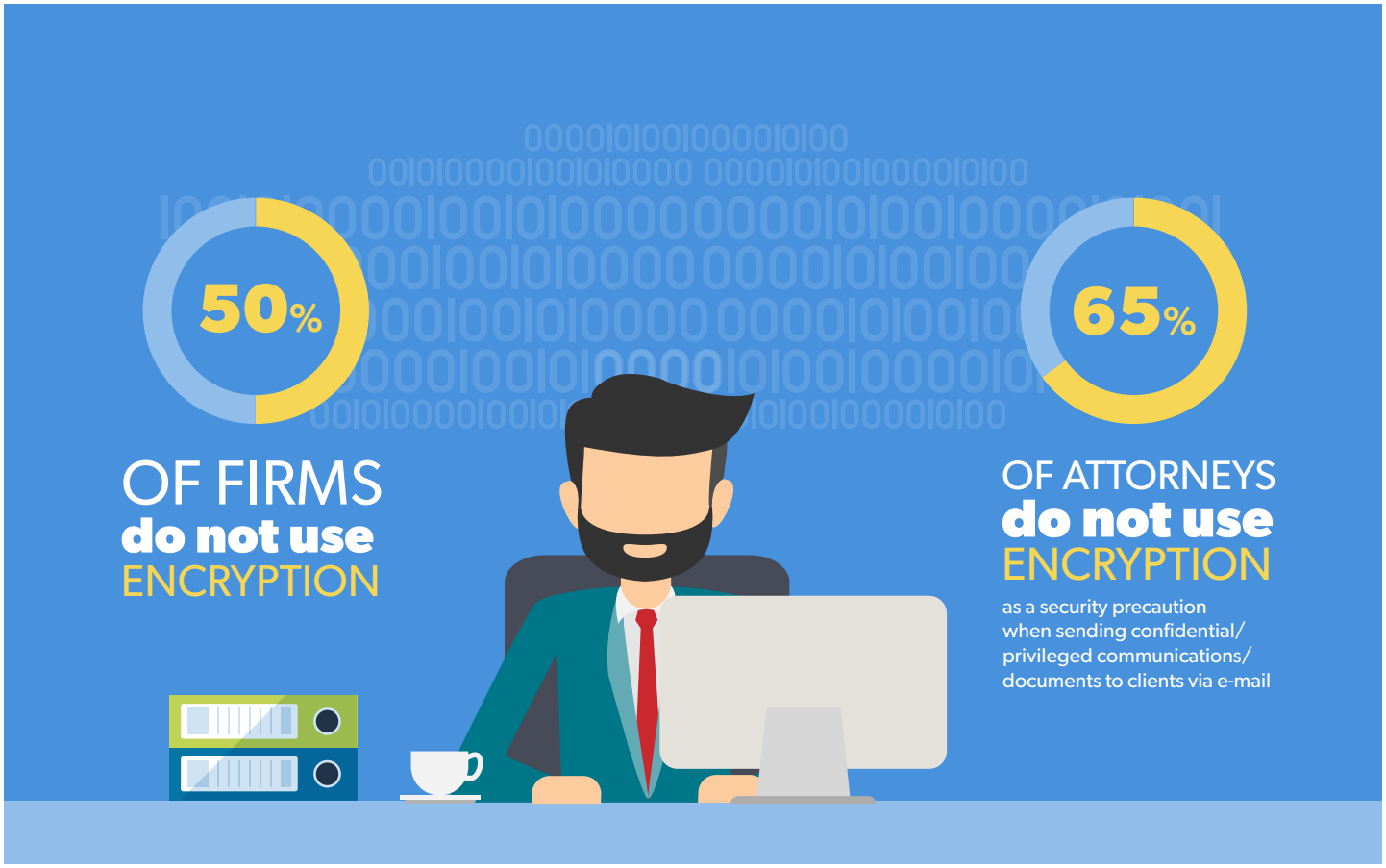
Additionally, not all law firms need a system of restricted access. Only create one if you actually believe it is necessary. Aside from making you much easier to hack (those more likely to have restricted access credentials are frequently targeted[15]), using cybersecurity as just another way to reinforce your office's social structure is a recipe for disaster.

12 Enterprise Information Security Standards: Data Classification, STATE OF MASS. EXEC. OFF. ADMIN. & FIN., (March 6, 2014), http://www.mass.gov/anf/research-and-tech/cyber-security/.

13 See e.g. 45 C.F.R. §§ 164.302-164.318 (2015).

14 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information, U.S. INTERNAL REVENUE SERVICE, 44-112, available at http://www.irs.gov/pub/irs-pdf/p1075.pdf (discussing cybersecurity requirements) (last viewed April 5, 2015).

15 Russell Brandom, Spy Group Stole Business Secrets Over Compromised Hotel Wi-Fi, THE VERGE (Nov. 10, 2014, 8:58 AM), http://www.theverge.com/2014/11/10/7185671/spy-group-stole-business-secrets-over-compromised-hotel-wi-fi.



Step 3: Encrypt Your Data

Data encryption is no longer a 'nice to have' for law firms[16]. For reasons passing understanding, there are a lot of people out there (not just law firms) who don't encrypt their data.[17] If you follow every step of this checklist, but refuse to encrypt your data, your cybersecurity policy will be ineffective and your data will still be at risk.

Encryption methods and practices vary, however, based on your data's location:

Data at Rest

Where do you save your data? Whether on your mobile device, in your server, or stored in a cloud storage system, data at rest ALWAYS needs to be secure. As far as data you entrust to third parties, the security will be largely based on the third-party's terms of service (discussed below).

On the other hand, for the data you save on your server, office computers, or mobile devices, that data needs to be encrypted. Your cybersecurity policy needs to address *both* the location of your data storage and how the data is to be encrypted when at rest.[18]

16 Adam Clark Estes, How to Encrypt Everything, GIZMODO (June 5, 2014, 4:40 PM), http://gizmodo.com/how-to-encrypt-everything.

17 Joshua Poje, Security Snapshot: Threats and Opportunities in ABA TECHREPORT 2013 (ABA Legal Technology Resource Center 2013), available at http://www.americanbar.org/publications/techreport/2013/security_snapshot_threats_and_opportunities.html.

18 Alan Henry, Five Best File Encryption Tools, LIFEHACKER (Feb. 8, 2015, 8:00 AM), http://lifehacker.com/five-best-file-encryption-tools-5677725.

Data in Transit

How does your data get from one person to another? When your data is "in transit" is when your data is most vulnerable.[19] Whenever you're sending confidential data from one place or person to another, it needs to be encrypted from the moment you send it to the moment they receive it. This type of security is called "end-to-end encryption." [20]

One way to transmit confidential data is through a secure portal[21] such as Clio Connect.[22] Numerous email, file sharing and messaging services[23] also provide end-to-end encryption. Even if someone intercepts your data in transit, they will still have to crack your encryption in order to read it.

Data in Use

The only time your data should be unencrypted is when it's being used. Once no longer in use, you data should be encrypted immediately, regardless of any minor inconveniences that may result. Do not allow your confidential data to be used and saved unencrypted (e.g. saving an important document as a Word file on your desktop) simply because it's easier for the user at the time.

Remember: The data of 80 million people stolen in the Anthem hack was not encrypted,[24] for the sake of convenience.[25]

Make sure it fits your law firm:

Your data encryption policy will need to walk the extremely fine line between useful and secure. Never sacrifice security simply for the sake of convenience.[26] However, if your encryption inhibits your ability to function efficiently, it's probably time to reexamine your encryption policy.

19 See, e.g., Brian Focht, New Threats to the Attorney-Client Privilege Part 2, THE CYBER ADVOC. (Nov. 21, 2014), http://www.thecyberadvocate.com/2014/11/21/new-threats-attorney-client-privilege-part2/

20 End-to-End Encryption, WIKIPEDIA, http://en.wikipedia.org/wiki/End-to-end_encryption (last viewed April 5, 2015).

21 Client Portal, WIKIPEDIA, http://en.wikipedia.org/wiki/Client_portal (last viewed April 5, 2015).

22 For more information on Clio Connect, visit https://support.goclio.com/hc/en-us/sections/200598534-Clio-Connect-for-the-Firm.

23 See, e.g., Lisa Needham, Keep Your Data Safe While Skyping, Chatting, and Using Your Smartphone, LAWYERIST (Dec. 1, 2014), https://lawyerist.com/78673/data-security-skype-chat-smartphone/.

24 Danny Yadron and Melinda Beck, Health Insurer Anthem Didn't Encrypt Data in Theft, WALL ST. J., Feb. 5, 2015, available at http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560.

25 Amar Toor, Anthem Failed to Encrypt Customer Data Prior to Cyberattack, THE VERGE (Feb. 6, 2015, 5:21 AM), http://www.theverge.com/2015/2/6/7991283/anthem-hack-encrypted-data.

26 Mark Wilson, After Anthem Hack, What GCs Should Know About Encryption, FINDLAW (Feb. 6, 2015), http://blogs.findlaw.com/in_house/2015/02/after-anthem-hack-what-gcs-should-know-about-encryption.html.

Step 4: Require Strong Passwords

This step has two parts. The first should be obvious: require passwords. Any computer, laptop, device, app, or software system that interfaces with your client data *must* be password protected. MUST.

The second part: the passwords need to be *strong*.

This will not be easy.[27] For most people, passwords are the annoying aspect of cybersecurity they deal with every day – any inconvenience is amplified.

The result: we don't use secure passwords.[28] They're too short, only contain letters, and are easily remembered. We use the same one over and over across multiple sites. Worse, they're easily guessed by any hacker who accesses our Facebook page.[29]

A "strong" password[30] is:

1. At least 8 characters (although many experts recommend 12[31]);
2. A combination of character types (at least one lower case letter, one upper case letter, one number and one symbol; newer password systems also recognize spaces);
3. NOT a common word or phrase; and
4. Changed regularly.

Your cybersecurity policy should require strong passwords. They really are better, providing considerably more security[32] for your data. I strongly recommend using a password storage system[33] like 1Password (which conveniently integrates with Clio).[34] In addition to storing various passwords, these systems can be set to generate strong passwords for you to use.

Tip

Also consider implementing multi-factor authentication where available.[35] Multi-factor authentication is a means of sending user verification messages when your accounts are accessed from a new device, and are offered by many services you currently use, like Clio[36] or Gmail.[37] These tools offer multi-factor authentication for little or no cost.

Make sure it fits your law firm:

Passwords are pretty much universally hated, so expect resistance. Remember, regardless the security benefits, you're making your employees' day less convenient. Like anything, if the system is too difficult or inconvenient, people will find ways around it.

Also remember that people use passwords in many parts of their daily lives, so beware the unintended consequences[38] of your policy. The more complex a password has to be, the harder it is to remember. As a result, your employees may be more likely to use a password they already use (for many, many logins). Require everyone to change their passwords frequently. People will inevitably use the easiest password to remember (like "0000" then "1111" then "2222," etc. on a mobile device), or write them somewhere that other people have easy access to. Ensure that the consequences of this are clearly explained, and make it firm policy to use a password manager.

27 Jason Straight, Law Firms Aren't Immune to cybersecurity Risks, NAT'L L. J., (Jan. 26, 2015), http://www.nationallawjournal.com/id=1202716120611/Law-Firms-Arent-Immune-to-Cybersecurity-Risks.

28 See, e.g., Brian Focht, Stronger Passwords to Protect Your Practice [Infographic], THE CYBER ADVOC. (Nov. 20, 2013), http://www.thecyberadvocate.com/2013/11/20/stronger-passwords-infographic/

29 John Pozadzides, How I'd Hack Your Weak Passwords, LIFEHACKER (Dec. 16, 2010, 9:01 AM), http://lifehacker.com/5505400/how-id-hack-your-weak-passwords.

30 Kevan Lee, How To Create a Strong Password You Can Remember Later: 4 Key Methods, BUFFER (June 25, 2014) https://open.bufferapp.com/creating-a-secure-password/.

31 Safe and Secure: cybersecurity Practices for Law Firms, CNA, available at https://www.cna.com/ (search for "safe and secure"; select first item returned) (last viewed April 5, 2015).

32 Annalee Newitz, 9 Facts About Computer Security That Experts Wish You Knew, GIZMODO (March 4, 2015, 2:05 PM) http://gizmodo.com/9-facts-about-computer-security-that-experts-wish-you-k-1686817774 (discussing email correspondence from Alex Stamos, Yahoo's Chief Information Security Officer).

33 Roberto Baldwin, How To Protect Yourself Against Hackers (Or At Least Make It Difficult For Them), THE NEXT WEb (Sept. 3, 2014, 9:33 PM) http://thenextweb.com/insider/2014/09/03/protect-hackers-least-make-difficult/.

34 For more information about 1Password, visit https://agilebits.com/onepassword.

35 See Brian Focht, Multi-Factor Authentication: the Imperfect Tool You Need to Use, THE CYBER ADVOC. (Jan. 26, 2015), http://www.thecyberadvocate.com/2015/01/26/multi-factor-authentication-imperfect-tool-need-use/; Tony Bradley, Data Breaches Can Be Prevented With One Simple Solution, PC WORLD (Jan. 19, 2015) http://www.pcworld.com/article/2871241/data-breaches-can-be-prevented-with-one-simple-solution.html.

36 For more information on Clio's multi-factor authentication options, visit https://support.goclio.com/hc/en-us/articles/203756468-Advanced-Security-Features-in-Clio.

37 For more information on Gmail's multi-factor authentication options, visit https://www.google.com/landing/2step/.

38 Omer Eiferman, Millennials Don't Care About Mobile Security, and Here's What to Do About It, WIRED, http://www.wired.com/2014/09/millennials-mobile-security/ (last viewed April 5, 2015).

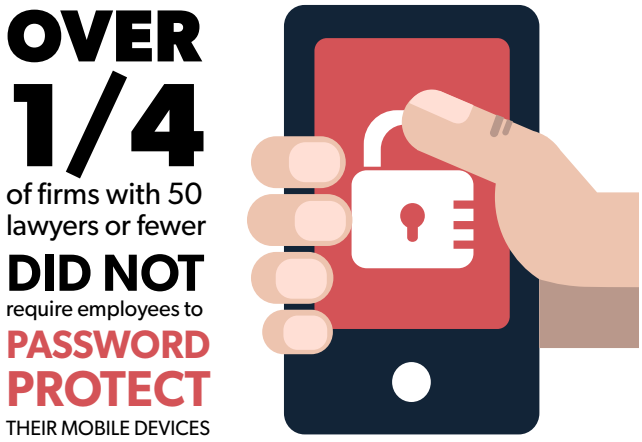
Step 5: Implement a BYOD Policy

We live in the era of the mobile device. [39]

Your attorneys and staff likely use their own devices for work, bringing with them a host of benefits[40] and potential risks.[41] No cybersecurity policy is adequate without addressing Bring Your Own Device ("BYOD"). Your BYOD policy must address the following issues:

- **Passwords** – They're required. Period.
- **Data encryption** – Every device must be able to encrypt data, and encryption must be active (*see* Step 3).
- **App Whitelisting** *(Optional)* – Allowing only certain apps for business use.
- **Mobile Device Management/Security Apps** *(Optional)* – At a minimum, your BYOD policy should require use of basic security tools like Find My iPhone[42] or Android Device Manager.[43] Additional security and management apps that allow remote locking and wiping of confidential information are useful, but can be seen as intrusive.[44]

Download a BYOD Policy Template



Make sure it fits your law firm:

People are quite attached to their personal devices, and studies indicate that people prefer[45] using their personal devices for work over a "company phone." However, an oppressive BYOD policy will quickly remind them[46] that you are treating their *personal* devices like company property.

Draft your BYOD policy with your employees in mind,[47] respect their privacy and seek their input. Remember, they're using a device *they* paid for to the benefit of *your* business.

39 See Brian Focht, Law Firms in a BYOD World [Slideshow], THE CYBER ADVOC. (Oct 17, 2014), http://www.wired.com/2014/09/millennials-mobile-security/.

40 See generally, Brian Focht, BYOD: Five Steps to Protect Your Clients and Save You Money!, THE CYBER ADVOC. (Aug. 19, 2013), http://www.thecyberadvocate.com/2013/08/19/byod-five-steps-to-protect-your-clients-and-save-you-money/.

41 See generally, Brian Focht, Awareness is the Key Ingredient for a Successful BYOD Policy, THE CYBER ADVOC. (Oct. 2, 2014), http://www.thecyberadvocate.com/2014/10/02/awareness-key-byod-policy/.

42 For more information about Find My iPhone, visit https://www.apple.com/icloud/find-my-iphone.html.

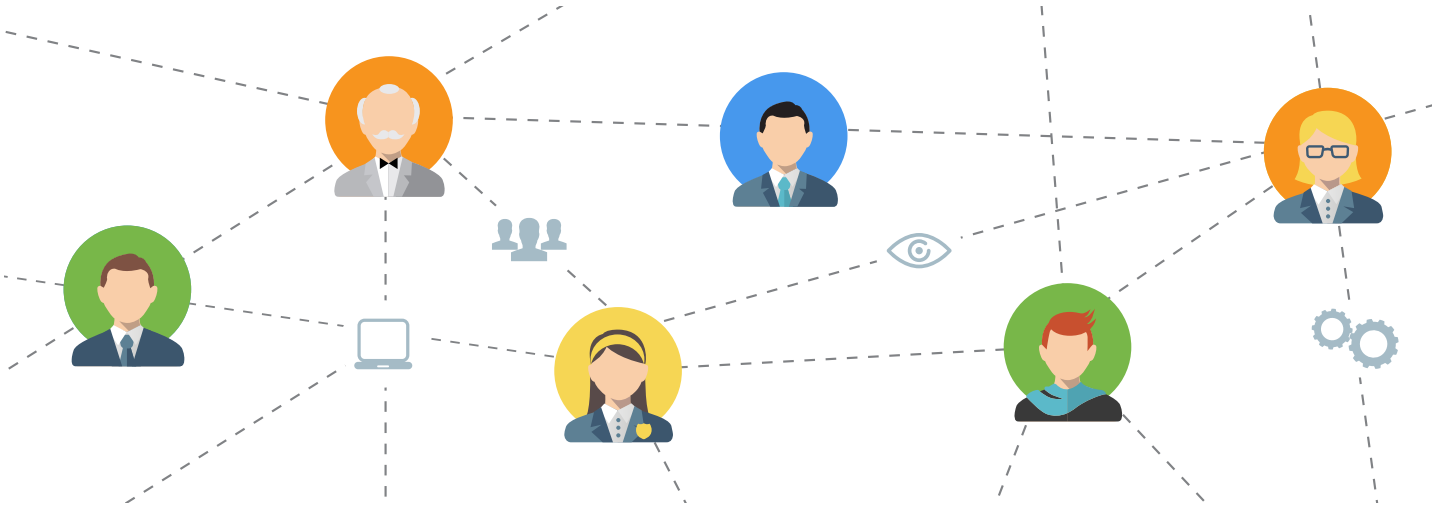
43 For more information about Android Device Manager, visit https://www.google.com/android/devicemanager.

44 Fixing the Disconnect Between Employer and Employee for BYOD (Bring Your Own Device), WEBROOT, 4-5, available at http://www.webroot.com/shared/pdf/WebrootBYODSecurityReport2014.pdf [hereinafter Webroot BYOD Report].

45 Susan Bassford Wilson, BYOD Requires BYOB: How to Handle the Challenges Inherent in a "Bring Your Own Device" Program in CONSTANGY, BROOKS, SMITH, & PROPHETE LLP CLIENT BULLetins (March 30, 2014), available at http://www.constangy.com/communications-511.html.

46 See Webroot BYOD Report at 4, supra note 44.

47 BYOD Security: What is the impact on employees?, WEBROOT, available at http://www.webroot.com/us/en/business/resources/infographics/byod-security-impact-on-employees (last viewed April 5, 2015).



Step 6: Create (and Regularly Update) a Network Map

You can't protect your data unless you know who has access to it. An efficient way for your IT manager to track access is an up-to-date network map.[48]

A network map is a visual representation of all the people and devices that have access to your network. All devices, including their IP address and other identifying information, are listed and linked to an authorized user. The view gives your IT manager a quick glance overview of your network, and its interconnected relationships.[49]

The network map itself includes all employees, attorneys, and third-party vendors. It should reflect any restricted access, as well as all third-party connections (e.g. including cloud storage vendors, IT contractors, and your accounting/practice management companies).

An updated network map has two primary purposes:

First, it allows your IT manager to ensure each connected computer or device has the proper updates and to fix security vulnerabilities. In the event of a data breach, you will be in a better position to identify the source of the breach.

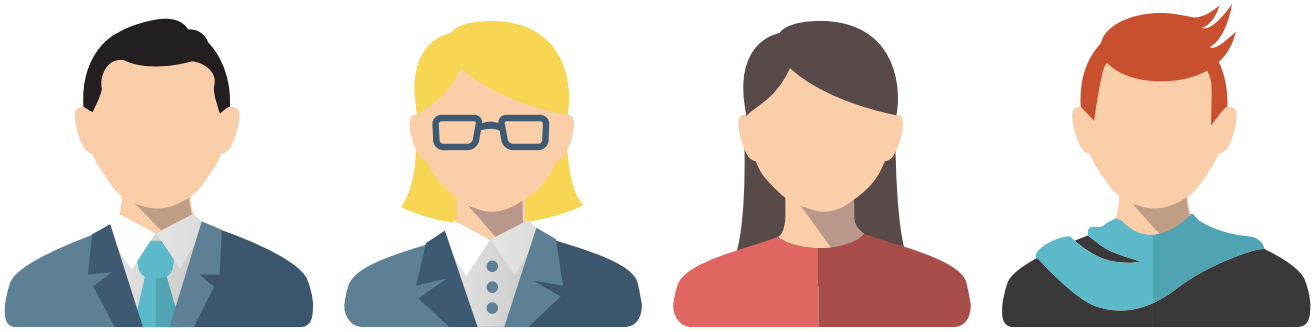
Second, it highlights vulnerabilities caused by expansion and modifications of your network. Frequently, when new network connections are added, existing cybersecurity protocols do not entirely protect the new connection. By keeping the network map updated, your IT manager can minimize any associated vulnerabilities.

Make sure it fits your law firm:

While the network map is important, it is important that you do not use the maintenance of the map as justification for being inflexible. Your network map should reflect the current status of your law firm, but cannot serve as a gatekeeper for change.

48 Network Map, TECHOPEDIA, http://www.techopedia.com/definition/4993/network-map (last viewed April 5, 2015).

49 Working With The Network Map, MCAFEE, http://download.mcafee.com/products/webhelp/4/1033/GUID-C9551648-E355-4C15-86A5-51AE76D79E51.html (last viewed April 5, 2015) (a list of resources for using a network map).



Step 7: Audit Your Third-Party Contracts

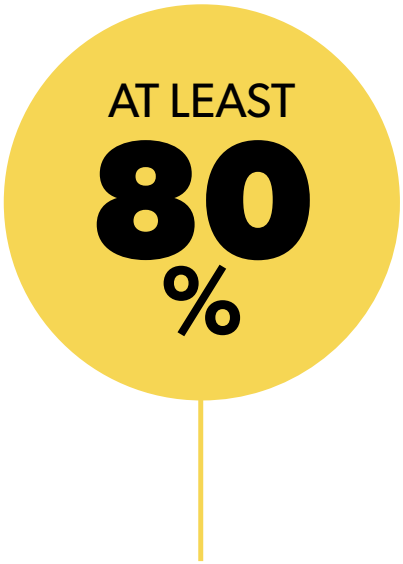
Your employees aren't the only people with access to your network. Every third-party vendor who connects to your network is a potential vulnerability, unless managed properly.[50]

Although some vendors who deal exclusively with attorneys understand the unique privacy issues lawyers deal with, most won't take it into consideration by default.[51] That's because most vendors do not deal exclusively with lawyers, particularly cloud storage and IT vendors.

You trust your vendors with information that you are legally bound to protect. Under the Model Rules of Professional Conduct, you're required to ensure the information remains protected[52] by your vendor. Your vendor's Terms of Service need to answer the following questions[53]:

- Who has access to your data?
  - Does every one of your vendor's employees have access? Just a few?
  - How does your vendor record attempts to access your data?
  - *Must meet same ethical standards applied to your law firm!*
- How can you retrieve data from your vendor…
  - If you terminate your contract with the vendor?
  - If your vendor goes out of business?
  - In the event of a break in continuous service?
- Will the vendor return or destroy all data on demand?
  - Will they guarantee it's in a universal format?
- How do they keep your data secure?
  - What types of encryption and firewalls do they use?
  - What duty do they have to notify you in event of a breach?
  - Who will be liable for any damages suffered by your client?
- What is their data backup system/policy?

Download a Vendor Audit Checklist



You will also likely have to ask questions based on your state's ethical rules. For example, can you obtain a complete copy[54] of any client's information in the event you haven't paid your bill?

Fortunately, many vendors understand that lawyers' needs are a bit different than the norm. Vendors will often allow you to negotiate parts of their Terms of Service.[55] However, *do not compromise*. If a vendor is unable or unwilling to modify their terms to meet your needs, don't use them.

Make sure it fits your law firm:

Relationships matter. It's likely that many of your vendors have been working with your law firm for quite some time. You and your staff are familiar and comfortable with your vendors.

If a vendor has provided excellent service, but cannot meet your requirements for handling confidential information right now, it doesn't mean they'll never be able to. Informing them of your specific needs might encourage them to improve. Until they do, however, you have a legal and ethical responsibility to take your business elsewhere.

50 Ajay Patel, The Secret to Secure Data in the Cloud? Know What You're Up Against, LAW TECH. TODAY (Sept. 30, 2014), available at http://www.lawtechnologytoday.org/2014/09/the-secret-to-secure-data-in-the-cloud-know-what-youre-up-against/.

51 See Carolyn Elefant, New York Report on The Cloud and Small Law Firms: Reasonable Advice But Wrong Solutions, ABOVE THE LAW (Jan. 6, 2014, 3:44 PM), http://abovethelaw.com/2014/01/new-york-report-on-the-cloud-and-small-law-firms-reasonable-advice-but-wrong-solutions/ (discussing the difficulty solo and small firms might encounter in negotiating terms of service).

52 See A.B.A. Comm. On Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008) (discussing lawyer's obligations when outsourcing legal and nonlegal support services).

53 Straight, supra note 27.

54 See, e.g., N.C. State Bar 2008 Formal Ethics Opinion 5 (2008) (discussing web-based management of client records).

55 Sam Glover, Terms of Service for Cloud Software Are Negotiable, LAWYERIST (Sept. 23, 2013), https://lawyerist.com/69916/terms-service-cloud-software-negotiable-cliocloud9/

54 See Lee Rosen, Are You Backing Up Your Life?, DIVORCE DISCOURSE, https://lawyerist.com/69916/terms-service-cloud-software-negotiable-cliocloud9/ (last viewed April 5, 2015) (discussing the consequences of being unable to recover lost data).

55 Mark Wilson, How to Survive After a Law Firm Computer Crash, FINDLAW (Feb. 24, 2015) http://blogs.findlaw.com/technologist/2015/02/how-to-survive-after-a-law-firm-computer-crash.html.

Step 8: Establish a Data Backup System

If your local server was hacked and you lost everything stored there, what would you do?

Your cybersecurity policy needs to provide for recovery from a cyber attack[56] as quickly as possible. Effective recovery requires an efficient and complete backup system.[57] Your IT manager will be responsible for setting up your data backup system by creating a data backup schedule and selecting your data backup locations.

Your Data Backup Schedule

Your data backup schedule determines what information is captured by your backup, and how frequently. The more frequent the backup process, the better – but it can be a drain on computer resources. All employees should know where to save data and business information in order to be captured by your regular backups. *Important, unencrypted data should never be saved to a computer desktop or mobile device without approval from the IT manager.*

Tip

Setting up a data backup system is also an ideal opportunity to make sure your data retention/destruction policy is up to date as well.[62]

Your Data Backup Location

Just as important as what data is backed up is where your data is backed up. Redundancy is the goal: you firm requires data to be backed up in multiple ways,[58] and in multiple locations.[59] Put it this way – if one significant event, like a fire or flood,[60] can destroy all of your backups, you your system is insufficient. Numerous cloud storage options[61] are available with multiple, redundant backups. (*Just don't forget to review the Terms of Service!*)

Make sure it fits your law firm:

Different law firms generate and store information in different ways. Make sure that your backups capture all of the valuable information you generate. Everyone needs to keep data in a location that the backup system will capture.

Getting hacked can result of theft or destruction of valuable information. Being unable to recreate the information due to insufficient backup system compounds the damage!

58 Jon Jacobi, The Absurdly Simple Guide to Backing Up Your PC, PC WORLD (Nov. 25, 2013) available at http://www.pcworld.com/article/2065126/the-absurdly-simple-guide-to-backing-up-your-pc.html.

59 See, e.g., William Peacock, The Cloud and Why Lawyers Should Give a Damn, TECHNOLOGIST (Jan. 22, 2013) http://blogs.findlaw.com/technologist/2013/01/the-cloud-and-why-lawyers-should-give-a-damn.html.

60 See, e.g., Nicole Black, Fire at Buffalo Firm Proves Value of Digital Storage, SUI GENERIS BLOG (March 13, 2015) http://nylawblog.typepad.com/suigeneris/2015/03/fire-at-buffalo-firm-proves-value-of-digital-storage-.html.

61 For a list of cloud storage options compiled by the ABA, visit http://www.americanbar.org/publications/law_practice_magazine/2011/september_october/popular_cloud_computing_services_for_lawyers.html.

62 Megan Zavieh, Sample Document-Destruction Policy, LAWYERIST (Jan. 21, 2014), https://lawyerist.com/71530/sample-document-destruction-policy/.

Step 9: Ensure The Physical Security of Systems and Facilities

Physical security is a huge, yet underappreciated component of cybersecurity.[63] Your network is only as secure as your office. And I'm not just talking about direct access to your server, either.

Information routinely used by hackers can be obtained frequently just by looking around someone's desk.[64] Passwords, social engineering information, your staff's personal information – all sit prominently on display.

Your cybersecurity policy needs to include an assessment[65] of your office's physical security. Threats can generally be grouped into three categories[66]:

1. **Environmental Threats**
   (such as fire, flood, hurricane),
2. **Human Threats**
   (such as direct access to servers, ease of entry), and
3. **Supply System Threats**
   (such as a power outage).

Download a Physical Security Checklist

Make sure you have a physical security program in place that addresses these threats. In addition, secure any lists of passwords or company employees.[67] Encourage your employees to secure anything containing personal information when they leave their workspace and NEVER leave login credentials and passwords out in the open.

Make sure it fits your law firm:

While you need to make sure that your data is safe from physical threats, you also don't want your office to feel like a police state. As with everything else on this list, you need to tailor your security to both the needs and the resources of your law firm.

63 See Larry Port, Cloud v. On-Premise Security, LAW TECH. TODAY (March 3, 2015), http://www.lawtechnologytoday.org/2015/03/cloud-v-on-premise-security/ (discussing the importance of physical security to any cybersecurity system).

64 Peter Giannoulis and Stephen Northcutt, Physical Security in SECURITY LABORATORY: IT MANAGERS - SAFETY SERIES (SANS Institute) http://www.sans.edu/research/security-laboratory/article/281 (last viewed April 5, 2015).

65 Cybersecurity and the Duty of Care, supra note 9.

66 Christian Malatesti, Physical Security in the IT Space, ENTERPRISE RISK MGMT., http://www.emrisk.com/knowledge-center/white-papers/physical-security-it-space (last viewed April 5, 2015).

67 Id.

Step 10: Provide Meaningful Education & Training

Reluctance to embrace cybersecurity policies and procedures can often be tied to a poor understanding of the importance of security policies and the consequences of getting hacked. Most cybersecurity training adequately teaches people the "how." However, it fails because it routinely ignores the "why."[69]

Awareness is the Key

One of the most critical elements of cybersecurity is awareness.[70] Your attorneys and staff need to think of cybersecurity as more than just an inconvenience. They need to understand that a successful cyber attack could shut down your law firm. They also need to realize how critical they really are to preventing an attack.[71]

Make sure they're aware of the threat, and aware of their significant role in detecting those threats.

Take Training Seriously

That's where training comes in. Set up a schedule for *mandatory* cybersecurity training. Then make the training two things no legal training session has ever been: interesting *and* useful.

Educate your staff about the importance of recognizing and reporting threats,[72] both the "how" and the "why." Include examples of social engineering and email phishing attacks.[73] Explain the importance of reporting suspicious incidents to the IT manager. Demonstrate the importance of each part of your cybersecurity policy using real life examples. Training needs to reinforce the concept that everyone is a stakeholder in cybersecurity.

Make sure it fits your law firm:

Training must be taken seriously by everyone in your law firm, particularly those at the top.[74] If your staff sees senior attorneys routinely skipping training sessions, it conveys that the training isn't truly important.

So get everyone there. Offer food. Really, free lunch might be the single best way to get attorneys to attend anything.[75] Training is incredibly important. Do whatever you have to do in order to ensure that your attorneys and staff take it seriously.

68 Burton, supra note 2.

69 Id.

70 See Focht, supra note 41.

71 Joseph Marquette, Biggest cybersecurity Threat to Law Firms is Not What You Think, ACCELLIS TECH. GRP. (March 5, 2015), http://accellis.com/biggest-cyber-security-threat-to-law-firms-is-not-what-you-think/.

72 See Rick Howard, When it Comes to cybersecurity, Look Past Your Employees, WIRED, http://www.wired.com/2015/03/comes-cybersecurity-look-past-employees/ (last viewed April 5, 2015).

73 Ben Weinberger, People + Access = Biggest Security Threat, LAW TECH. TODAY (March 20, 2015), http://www.lawtechnologytoday.org/2015/03/security-threat-people/.

74 Id.

75 No citation necessary. This statement is verifiable fact.

Step 11: Schedule Cybersecurity Audits

One of your IT manager's primary responsibilities is regularly testing your cybersecurity. These tests, cybersecurity audits, evaluate compliance with and effectiveness of your cybersecurity policy. Your IT Manager should perform both regularly scheduled and random audits.

Evaluate Compliance

The first component of a cybersecurity audit involves evaluating compliance with your cybersecurity policy. Your company's systems and software should be inspected regularly to ensure that all appropriate security measures are in place and properly updated.[76] Make sure security updates are installed and that anti-virus systems and email filters are functioning properly.

Evaluate Effectiveness

The second component of your cybersecurity audit evaluates the effectiveness of your cybersecurity through simulated cyber attacks. Your IT manager will simulate elements of different cyber attacks, including social engineering[77] and phishing attacks on attorneys and staff, to test vigilance and awareness.[78]

Your IT manager will also look for vulnerabilities in your security using penetration testing. A Penetration Test (or a "Pen-Test") basically involves trying to hack into your own network.[79] Simulating commonly used cyber attack techniques, a Pen-Test will let you know where the vulnerabilities exist in your network.

Evaluate Your Cybersecurity Policy

Don't forget to perform regular audits of your cybersecurity policy itself. Update your policy where necessary to incorporate new information and modify parts not working well. Keep an open mind and always look for things you can improve.

Make sure it fits your law firm:

There can be a fine line between testing an employee's vigilance and outright harassment. Your IT manager's job is to enforce the cybersecurity policy. However, you need to make sure that testing your employees doesn't become a distraction. This is one area where supervision of your IT manager is critical.

76 See, e.g., Straight, supra note 27.

77 Rick Lutkus, Information Security Threat: Social Engineering and the Human Element, LAW TECH. TODAY (March 11, 2015) http://www.lawtechnologytoday.org/2015/03/information-security-threat-social-engineering-and-the-human-element/.

78 Howard, supra note 72.

79 A Pentest's Benefits, REDTEAM PENTESTING GMBH, https://www.redteam-pentesting.de/en/pentest/benefits/-benefits-of-a-penetration-test (last viewed April 5, 2015).

Step 12: Prepare a Response Plan

The reality of cybersecurity is that you can hope for the best, but you need to prepare for the worst. What if the *worst* happens? What will you do if your security, no matter how strong, isn't enough? Your cybersecurity policy must include directions for preparing a response plan.

Tip

I strongly recommend creating a separate response plan for each type of confidential data identified in Step 2. One reason response plans fail is because they don't provide clear, specific instructions. Separate response plans let you address steps not applicable to other types of data.

Your response plans should answer the following questions:[80]

1. Who will be notified?
   - All clients?
   - Only clients whose information *may* have been accessed?
   - Only clients whose information you *confirm* have been accessed or stolen?
2. What is your notification timeframe?
   - Do you rely on the maximum time allowed by law (30 or 60 days in most cases)?
   - Do you decide on a case-by-case basis?
3. What documentation must be kept regarding the breach?
   - The minimum required by law?
   - The minimum necessary to present to an ethics committee?
   - Should you keep different documents based on the clients affected?
   - Does your cybersecurity Insurance have certain requirements?
4. Who is authorized to speak about the breach?
   - To clients?
   - To law enforcement?
   - To the press?
5. Who is authorized to make critical decisions?
   - About the investigation?
   - About retaining documents?
   - To authorize the IT manager to proceed through steps to restore systems?
   - What if the one person you've designated is unavailable?

Download a Sample Response Plan

Plan appropriately for the situation. Prepare for a situation when your major decision makers may be unavailable. Your IT manager should know who is next in the chain of command.

Too often, response plans fail due to poor design or poor implementation.[81] So coordinate the response plan across your business, and keep your response plan up-to-date.

Make sure it fits your law firm:

Understanding your law firm's internal dynamics is critical to creating appropriate response plans. Internal lines of communication, clear objectives, and a thorough awareness on the part of your staff should be your primary concern.

BONUS TIP: WRITE IT DOWN AND ENFORCE IT!

You could follow these steps to a proverbial "T," but you're just wasting your time if you don't write it down and properly enforce it.

A Written Cybersecurity Policy...

Put your cybersecurity policy in writing, so that you *and* your employees can read it.[82] Writing it down gives you the opportunity to review it as a whole. Is it reasonable? Is it understandable?

... That Applies To Everyone!

Then, empower your IT manager to enforce it. Universally.

There can be no exceptions for anyone at your law firm, especially for those at the top. Exceptions indicate that you don't really take cybersecurity seriously. Moreover, they can actually make you more vulnerable.[83] Your cybersecurity policy isn't just important – it's critical. Don't do anything to jeopardize it!

Make sure it fits your law firm:

Your cybersecurity policy must be flexible and workable. Don't be afraid to change it to reflect your law firm's unique situation or experience. Get input from every level when drafting it, and actually *listen* to the input.

Your cybersecurity policy is only as strong as the proverbial weakest link – an employee who feels unimportant can be your worst nightmare. However, an employee who feels included and valued, understands the risk and the consequences of an attack, uses a strong password, has been trained to spot and report suspicious behavior – who knows how important they are to the success of your cybersecurity policy – is your law firm's best defense against a cyber attack.[84]

80 Jody R. Westby, Cybersecurity & Law Firms: A Business Risk, LAW PRAC. MGMT., July/August 2013, available at http://www.americanbar.org/publications/law_practice_magazine/2013/july-august/cybersecurity-law-firms.html.

81 Tucker Bailey et al., How Good is Your Cyberincident-Response Plan?, MCKINSEY & CO., http://www.mckinsey.com/insights/business_technology/how_good_is_your_cyberincident_response_plan (last viewed April 5, 2015)

82 See, e.g., Burton, supra note 2.

83 Top 10 Tips for Educating Your Employees About cybersecurity, KASPERSKY LABS, 6, available at http://go.kaspersky.com/rs/kaspersky1/images/Top_10_Tips_For_Educating_Employees_About_Cybersecurity_eBook.pdf (last viewed April 5, 2015).