

Law Firm Cybersecurity Survival Guide

What Your Firm **Must Do** to
Safeguard its **Data** and its **Clients**

By Dennis Dimka

About the Author

In 2012, Dennis Dimka, Chief Executive Officer of Uptime Legal, made a decision that has brought unparalleled results for the company and its clients. That decision was simple, Uptime would focus exclusively on providing cloud services to small and



mid-size law firms. Why take such a risk? He believed law firms required a unique set of services and product commitment. He was right. Today, Uptime provides hosting, software, and support to more than 400 law firms and thousands of legal professionals in North America.

Uptime is truly agnostic in its approach to legal software. The experience gained from working with leading legal applications is significant. This eBook is dedicated to all those firms struggling to understand how best to approach cloud computing and evaluate their choices.

CONTENTS

Part I - General Cybersecurity Practices	5
Chapter 1 - Compliance & Security Standards	7
Chapter 2 - Security Policies.....	8
Chapter 3 - Firewalls & Intrusion Prevention.....	10
Chapter 4 - Software Security Patches	12
Chapter 5 - Educating Your Firm	14
Chapter 6 - Encrypting Your Devices	15
Part II - Email Security	17
Chapter 7 - Email Archive	19
Chapter 8 - Email Encryption	20
Chapter 9 - Mobile Device Management (MDM)	21
Part III - Cybersecurity in the Cloud.....	22
Chapter 10 - Use a Reputable Legal Cloud Service Provider ...	24
Chapter 11 - Ensure Your Data Stays Yours (and Stays in the US)	25
Chapter 12 - Demand Bank-Grade Security.....	26
Chapter 13 - What If Your Cloud Provider is Served with a Subpoena?.....	27
Chapter 14 - Two-Factor Authentication (2FA) and Restricted Access	28
Chapter 15 * Onsite Cloud Backup	29
Appendix - Ransomware.....	30

Cybersecurity breaches and threats consistently make the headlines these days. And it's not just media sensationalism. Information security threats are more prevalent now than ever.

Every business should take reasonable care to protect its data. Law firms, possibly more than any other industry, have a mandate to educate themselves on information security and to take every reasonable measure to keep their firm and their clients' data secure.

Think of all the sensitive data your firm has for its clients:

- » Sensitive financial data;
- » Personally identifiable information;
- » Family information;
- » Health and medical records;
- » Intellectual property;
- » Trade secrets;
- » And on and on.

According to Bloomberg, roughly 80% of large law firms have experienced some sort of data breach.

Law firms are especially attractive to cyber-criminals due to the very sensitive, and potentially valuable information that a law firm likely has.

Moreover, because many companies have robust security measures, law firms are viewed as the soft underbelly of cybersecurity. Cyber-criminals looking to access sensitive data target the company's law firm rather than the company itself because of the easier access.

Even small firms and solo practices are appetizing targets to seasoned hackers and wanna-be's alike (and there are plenty of both.)

For this reason, every law practice has an ethical and professional duty to actively work to keep its client data safe.

The state ethics rules pertaining to lawyers require that law firms take "reasonable measures" to protect client confidentiality. With the rise in data breaches and cyber-intrusion, it is incumbent upon law firms to take substantial efforts to protect client data.

The good news is that achieving information security isn't out of reach, even for small law firms with limited budgets. You don't necessarily need to retain an expensive cybersecurity consulting firm to plug the holes in your firm's information security or implement good cybersecurity practices.

In this eBook we'll cover the full spectrum of potential security threats: and what your law firm should do to address each potential risk, a process known in the security world as hardening.

We'll explore general computing and technology measures to employ, as well as measures to have when moving your law firm to the cloud.



PART I

GENERAL CYBERSECURITY PRACTICES



In Part I, we'll explore universal and general security measures that should be part of your law firm's DNA. Whether you're a solo practitioner or an AMLaw 100 firm, whether your firm owns and manages a sophisticated on-premise IT infrastructure or lives entirely in the Cloud, these are the areas your firm must address to remain secure.

Compliance & Security Standards

The best place to start when thinking about cybersecurity for your law firm is information security standards and frameworks.

When it comes to keeping any organization's data secure from hackers, viruses and other malevolent forces, a doctrine has already been developed (and is regularly updated). Thankfully, we don't need to reinvent the wheel here.

Acknowledging the need for a universal and consistent approach to cybersecurity, a number of organizations have developed specific *security standards*, or frameworks for implementing and managing cybersecurity.

This is a good thing, as it eliminates the need for every organization to evaluate threats and develop plans to protect against them. And—it provides a prescription for organizations and technology professionals to follow, so we're not all left making our best guesses when it comes to how to keep our data secure.

There are many well-known, suitable security standards used by the information technology industry, though (arguably) the two most well-known and often used are the **ISO 27001**, and the **NIST Security Standard**. Most of the best-practices

we'll explore in this book are based on the latter.

Many third-party regulations, such as HIPAA, SOX and PCI compliance borrow heavily from or simply refer to one of these standards, such as NIST, as to how to do your cybersecurity due-diligence.

Some industries, such as healthcare and financial services, are formally regulated (by bodies such as HHS and the SEC).

Law firms are regulated by ethical standards, each prescribed by state professional regulatory agencies, courts, and/or bar associations.

Unlike healthcare and financial services, though, there are not specific technical requirements on data protection in legal. Though, firms handling sensitive financial or health information may be covered by HHS and SEC regulations.

Regardless, a law firm should employ the same levels of security diligence that other regulated industries do. After all— isn't your client data just as crucial?

Security Policies

Let's start with the basics. As prescribed in the NIST security framework, it's important to have some basic computer security settings applied across your firm, from your firm's servers, to its private cloud to its desktops and laptops.

These aren't rocket science, but are unfortunately often overlooked, or not put into practice.

We recommend the following settings be applied *universally* and *consistently* across your entire firm. These simple settings can be centrally defined, applied and administered with a tool built-in to Micro-

soft Windows Server, something called a *Group Policy*.

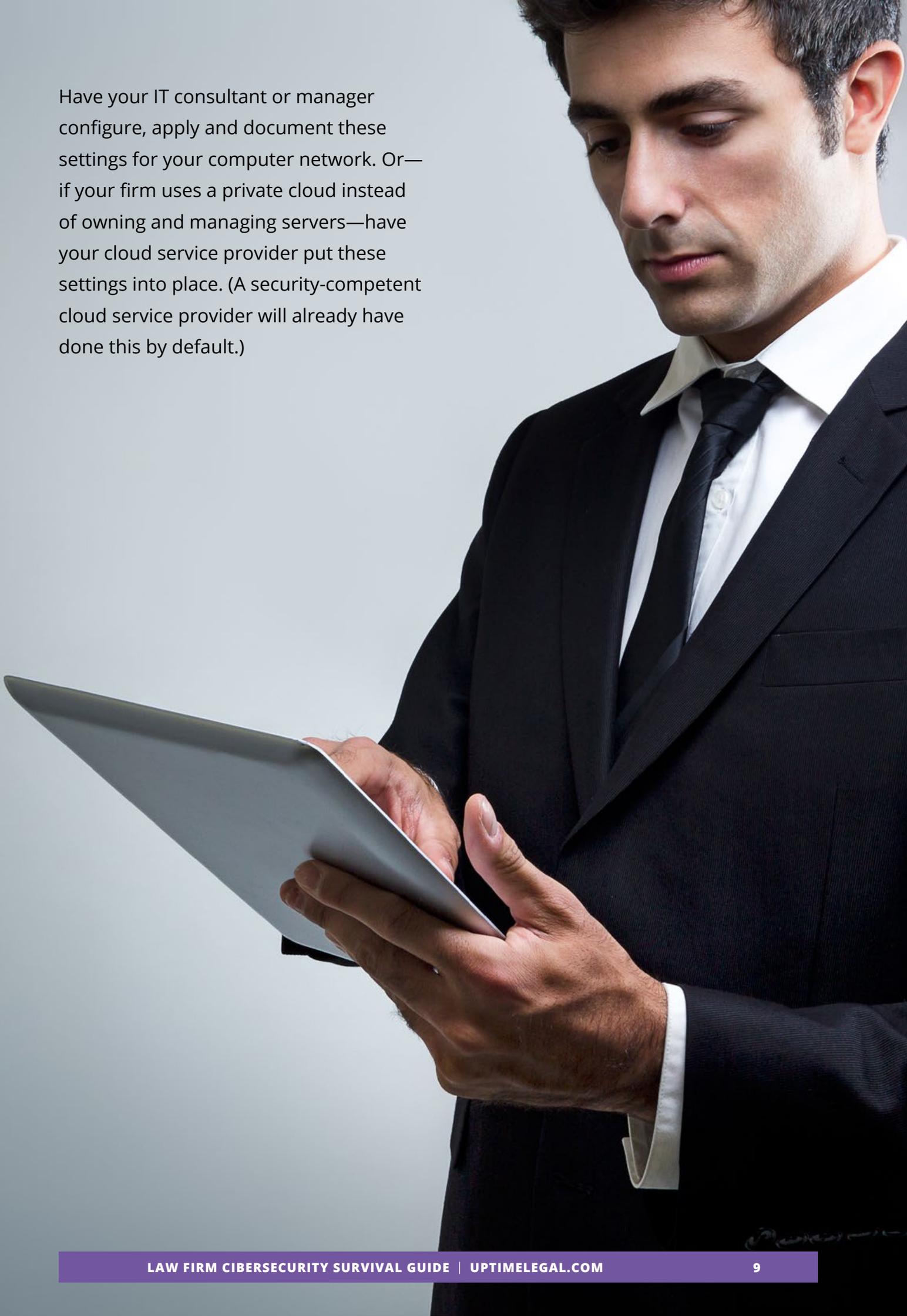
A Group Policy is where you (or your IT professional) can define universal settings, from password requirements to what the user's desktop looks like, in one place that will be uniformly applied to all computers within the law firm.

These settings will enforce basic security measures: Settings like password length, how unattended computers will automatically lock and how often users should change passwords. They're easy-to-implement but go a long way to securing your law firm. (Think of these as the low-hanging fruit of cybersecurity.)

Security Policies & Settings

SETTING	CONFIGURATION	DESCRIPTION
Password Complexity	Complex	Enforces complex passwords to prevent dictionary attacks.
Password Username	Enforced	Password cannot contain a portion of the username or full name.
Password History	Enforced	Cannot re-use the same password.
Idle Timeout/Lock	Enforced	Computers lock after 20 minutes of inactivity.
Maximum Password Age	6 Months	Users are required to change passwords every 6 months.
Failed Logins	10	Failed login attempts before the user's account is locked.

Have your IT consultant or manager configure, apply and document these settings for your computer network. Or— if your firm uses a private cloud instead of owning and managing servers—have your cloud service provider put these settings into place. (A security-competent cloud service provider will already have done this by default.)



Firewalls & Intrusion Prevention

Another cybersecurity 101: Have a firewall.

A firewall is what stands between your law firm's computers (and the information on them) and the rest of the Internet, which is a wild-west of cyber-criminals, hackers viruses and more. And your firm should have one.

Your law firm's firewall acts as the bouncer between the public internet and your private network.

A firewall will inspect every packet of data coming into (or leaving) your private network to make sure it *should* be coming in or out. It does this by inspecting the data within every packet and comparing it to known attack patterns.

For instance, a firewall knows what a particular cyber-attack looks like, from an intrusion attempt, to a Denial-of-Service (DoS) attack, to potential ransomware attacks (more on Ransomware later in this book). And when a firewall does its job—it will detect these and block them before they enter your network.

This is why it's important to not only *have* a firewall, but to actively *manage* it and keep it up-to-date.

Just like antivirus software must be routinely updated, your firewall needs constant updates to protect against the latest threats.

Beyond updates, a competent professional should routinely review your firewall's activity logs to spot threats when they occur and intervene as necessary. This can be done by hiring an IT consulting firm, or, if your firm has moved its practice to a competent private cloud platform, the cloud service provider will manage this for you.

Most commercial manufacturers of firewalls, such as WatchGuard and SonicWall, provide ongoing updates to their firewall's software to protect against the latest threats. They'll usually provide this in the form of an annual subscription. While this is an extra cost, don't chintse here. Pay the nominal fee to keep your information protected. This is a basic due-diligence item that can mean the difference between being hacked and staying secure.

A final note: There's sometimes a misconception that your organization, be it a law firm or something else, isn't "interesting enough" to be the target of hackers.

And that therefore security measures like implementing a firewall are "overkill".

Don't be fooled.

Over half of all hack attempts perpetrated across the Internet *aren't* necessarily targeted.

Hackers and automated tools scour the internet looking for unprotected hosts, akin to a car thief working a parking lot looking for unlocked cars.

And not having the firewall is the equivalent of leaving your car unlocked with the keys in the ignition.



Software Security Patches

Now that we have the perimeter of your law firm's network protected with a firewall, it's time to address the computers themselves.

Computer *security patches* are simple updates, developed and distributed by the manufacturer (such as Microsoft for Windows or Apple for MacOS) that protect against the latest threats and patch security vulnerabilities found within computer operating systems.

Routinely applying security patches is another easy-to-do security precaution that goes a long way.

The caveats?

- » You must regularly and reliably check for and apply these security updates.
- » You must run a *supported Operating System*.

Eventually companies like Microsoft will declare an older Operating System end-of-life, or out-of-support. This doesn't mean your old version of Windows will stop working on this date, but it *does* mean that they will stop patching security holes in the end-of-life OS.

This means any new vulnerabilities found in your old version of Windows will *not* be

Here are the basics: Companies like Microsoft and Apple make Operating Systems like Windows and MacOS. They do their best to make their OS's secure from cyber-threats. But inevitably, their OS's are imperfect, and sophisticated hackers will find vulnerabilities within them.

Operating System makers like Microsoft are constantly finding these security holes and patching them by releasing updates and fixes.

And, they make these updates automatically available to their customers (you).

patched, and will remain an open threat to your firm and your client data.

It's worth emphasizing that running an old, unsupported version of Windows is potentially the biggest cybersecurity mistake your law firm can make.

Take Windows XP, for example, which was classified as end-of-support April 8th 2014 (after a great 12-year run). Some law firms took a laissez-faire attitude and

continue to run Windows XP on their desktops. Meanwhile, new security exploits were found and developed for Windows XP every day, and Microsoft was no longer obligated to fix them.

In May 2017, a new version of ransomware, dubbed “WannaCry”, popped up on many Windows XP machines, taking advantage of a vulnerability. This affected thousands of machines, including the hospital system in the UK. Effectively, this malware disabled machines and halted businesses, losing them significant revenues, all because they were using an unsupported operating system.

Microsoft isn't to blame here, businesses that don't upgrade are.

Continuing to run out-of-date Operating Systems like Windows XP is potentially the biggest cybersecurity a law firm can make.

So, be sure to run a supported operating system.

And be sure to routinely update and patch your servers and your desktop and laptop computers.

Have a qualified IT professional do this for you, or, in the case of a private cloud, the cloud service provider will manage this for you.



Educating Your Firm

Before we go any further, it's important to discuss the ongoing *education* of your entire firm.

No, every person in your firm doesn't need to be an information security expert. But a little education goes a long way.

Start by declaring your firm's commitment to keeping its data (and your clients' data) secure. Let everyone in your firm know that you take cybersecurity very seriously, and that your firm will be implementing practices and protocols to keep your data secure. This will not only inspire confidence within your team but will put some context to the firm's new password policy or to your firm's adop-

tion of Two-Factor Authentication (more on 2FA later).

Next, make the education of your firm a *continuing* education.

You have regular all-company meetings, right?

A handful of times per year, take the opportunity to bring your firm up to speed. What new security measures will you be putting into place? What suspicious emails should everyone be on the lookout for? Oh, and—everyone knows not to open emails from sources they don't know, *right?*

When it comes to cybersecurity, ignorance is no excuse, and that applies to every single member of your law firm.



Encrypting Your Devices

We've covered how to secure your firm's network's perimeter. We've covered how to patch your computers and the importance of educating your team. Next, another fundamental is *encrypting your individual computers and mobile devices*.

First, on encrypting computers.

Encrypting the hard drive of your staff's computers is important. Even if your firm uses cloud-based software or runs its legal software in a private cloud, there's still some chance that sensitive client data will find itself to the local hard drive of your employee's desktop or laptop. Some scenarios include:

- » Your staff members may copy files to their local hard drive to work on offline.
- » Your staff members probably have Outlook setup in cached mode on their laptops, so they can access their inbox while offline.

Now imagine an staff member accidentally leaving that laptop unattended at an airport or hotel. Or imagine someone breaking into your law office and stealing one or more desktop computers. For this reason, even if you store your data in the

cloud, it's a good practice to encrypt the hard drive of every computer.

Windows. On Microsoft Windows, you can enable *BitLocker* to encrypt the hard drive of your computer. This is a good idea for each of your desktops, and a virtual must-do for laptops and Windows tablets. BitLocker will encrypt the hard drive such that data on it cannot be retrieved without the encryption key.

Mac. On a Mac computer, you can use *FileVault* to encrypt the computer's hard drive. Like BitLocker, FileVault will keep anyone who doesn't have the encryption key from accessing the contents of the computer's hard drive.

Modern encryption is virtually unbreakable, and built into the Operating Systems you use every day. Do yourself and your firm's security a favor - take advantage of them.

Mobile devices. Your mobile devices are equally important to encrypt. Likely every staff member at your firm accesses email on mobile devices, and probably also downloads and views attachments that may include sensitive information. Thus, it's important to ensure your mobile devices are encrypted.

Hopefully, you are already using encryption on your phone.

If you have to enter a pin number to access your phone's contents, you have encryption!

Surprisingly, many people, lawyers included, do not have encryption set up on their phones, despite the sensitive information available inside.

A popular excuse is, "It's a pain" or "I don't have anything interesting on my phone." But, as you know, law firms have sensitive client data on their devices – information that *must* be protected.

So, let's ensure you have encryption set up.

iPhone. Go to settings > Touch ID & Passcode to create a password if you do not have one. Once you've set a passcode, scroll down to the bottom of the Passcode settings page. You should see a message that says "Data protection enabled." Then, you're all set.

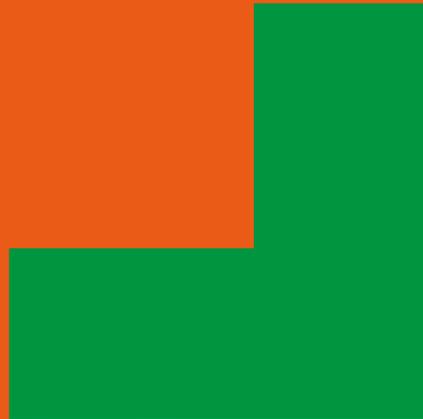
Android. To get started, go to Settings > Security > Encryption > Screen lock. Select the PIN option and enter a PIN. Next, use the settings menu to open the encryption screen below by following Settings > Security > Encryption > Encrypt tablet or Encrypt phone.





PART II

EMAIL SECURITY



Email is a major communication hub for all organizations, and law firms are no exception. Email is a massively useful tool to law firms, but is also where a lot of the cybersecurity threats live.

From virus proliferation, to phishing and other fraudulent activities, if there's going to be a security breach within your law firm, odds are it will happen with email.

So, Is regular email service good enough for law firms? To answer this question, first we must review the unique obligations of law firms to their clients:

- The ethical obligation to keep client's information safeguarded and secure;*
- The obligation to avoid intended or accidental disclosure of sensitive information;*
- The inherent obligation to maintain copies of relevant communications with or regarding a client or case, including email in its original form.*

Clearly, the conclusion to the question is regular email service good enough for law firms is: No.

So, if a garden-variety email service isn't acceptable for the practice of law, what is? What extra functionality does a law practice require? In Part II, we'll explore the specific tools a law firm and how each one maps back to our list of legal obligations.

Email Archive

By default, using “standard” email, users send and receive email, and delete emails when they don’t want them anymore. Once a deleted email goes past the backup retention policy, that email is gone forever. For a law firm that potentially needs to access old email records indefinitely, this does not suffice.

Email Archive is a system that effectively creates a copy of every email sent or received by the law firm (and any person within it) and saves this email in a separate, searchable database.

This gives the firm’s administrator or partners the ability to search the database and find every email ever sent or received, regardless of what the end-user ultimately did with the email.

Imagine a rogue staff member: They’re sending and receiving emails that they should not have, maybe to a client, maybe to some other outside party. But, they cover their tracks and delete every email they’ve sent or received. With “standard” email, you’d be hard pressed to ever retrieve these emails again, especially after they’ve exceeded your email’s backup/retention cycle.

Or, in the alternative, imagine a simply unorganized staff member: One that is not good about saving and organizing important emails. Suppose you need to retrieve an email they sent or received years later.

In both of these cases the odds of finding the emails you need are slim to none. With an Email Archive system, you’re no longer at the mercy of how good (or bad) your staff are about saving emails.

And—any system that relies on your human employees never making a mistake is a fundamentally flawed system anyhow. With an Email Archive system, every email that anyone in your firm ever sends and receives will exist in a separate database that you can search, any time.

Email archive is a critical feature for any law firm, regardless of practice area.

Email Encryption

But what about securing the actual *content* that your firm sends by email?

Email is inherently unencrypted (and un-encryptable). The fundamental nature of the Internet protocols used to transport email (namely: SMTP) precludes the ability to encrypt email messages. Theoretically, emails can be intercepted in transit, creating a serious problem for the privacy and security of email messages sent and received by law firm personnel.

Think of the kinds of email you send to clients, colleagues, and other parties. Full of sensitive information, in the email body and in attachments. Natively, email is fundamentally insecure and ripe for a security incident.

Email Encryption is a system where sensitive email sent by the law firm is encrypted *before* being sent to the recipient.

But didn't we just state that email is un-encryptable?

Yes—so to get around this limitation, Email Encryption solutions essentially bypass regular email transit altogether.

When the law firm sends a sensitive email, the Email Encryption system intercepts the message *before* it enters the

public Internet, and in its place, sends an email message to the recipient, informing him of a secure message that he must click a (secure) link to read. The link takes the recipients to a web page via HTTPS (which is encrypted), once authenticated by some means (often a password or CAPTCHA code).

Email Encryption systems are typically policy-based, which means the system will intelligently deduce which emails should be considered sensitive due to the content, including credit card numbers, social security numbers, healthcare/HIPAA related information, and so forth.

This kind of policy-based email encryption is required or strongly recommended by some third-party regulators, as we discussed earlier. We believe that law firms, regardless of a regulatory mandate, have the obligation to implement legal-grade email, with encryption, across the board.

Mobile Device Management (MDM)

Finally, to wrap up our email security strategy, we come to Mobile Device Management. MDM, as its often abbreviated, is a system that manages every mobile device (phone and tablet) used in your firm.

In this day and age of Bring-Your-Own-Device (BYOD), and everyone bringing their own tablet and smart phone to work. Mobile devices are a huge potential security hole for your law firm. Think of it, dozens of your staff members sending and receiving email and client documents from their mobile devices—unchecked.

Mobile Device Management is a system that controls and manages every device used in your firm. While you can procure an MDM service from anyone, we recommend that the provider of your Exchange email service also provide Mobile Device Management.

How this works: When an employee of your firm first goes to connect to their work email on their smart phone, whether it's a firm-provided phone or their own personal smartphone, the MDM service will apply its security policies and management to the phone.

The user must agree to these security policies (or forego connecting to work email). Once they do, you, the firm has the ability to enforce security policies such as encryption and remote wipe capabilities.

Suppose (again) that an employee goes rogue. Or that one of your attorneys loses their phone somewhere. This phone is almost certainly connected to their work email which has tons of potentially sensitive information on it. With Mobile Device Management: You can enforce a lock screen that would prohibit others from spelunking the depths of the phone. Or you can remotely wipe, or erase, all data on the phone without having it in your possession.

Especially when you consider that rogue employees and lost devices are among the top security threats to law firms: Mobile Device Management is a critical component of your cybersecurity plan.



The image features three large, stylized L-shaped blocks arranged around the text. A blue block is on the left, an orange block is on the top right, and a green block is on the bottom right. The text is centered in the middle of the page.

PART III

CYBERSECURITY IN THE CLOUD

Cloud computing adds a new dimension to cybersecurity for law firms.

The cloud is rapidly transforming the way we do business and who we share our confidential client data with. On-premise IT infrastructures are costly burdens to large and small law firms alike, so it's no wonder that many firms are turning to the cloud to host their applications, documents and email.

Perhaps no industry more than the legal profession must consider security, privacy and ethical issues when moving to the cloud. Unfortunately, not all clouds are created equal. With security and a law firm's ethical obligations at stake, in Part III we explore the things your firm must do to stay secure when using a private cloud to host your law practice.

Use a Reputable Legal Cloud Service Provider

A Private Cloud may very well be the easy-button for turn-key cybersecurity. Unfortunately, not all clouds are equated equal.

Some so-called cloud service providers are new to private cloud hosting. Many local IT service companies, losing business every month to the cloud, have launched their own cloud offering: a “me too” approach to stop the hemorrhaging. Many of these small, local IT companies lack the experience required to build and manage a comprehensive cloud infrastructure.

Other cloud service providers have anterior focuses. For example, software companies eager to capitalize on cloud computing by quickly putting together their own private cloud offering.

Law firms simply cannot afford to gamble with their data on an untested, lesser-known provider. The cloud service provider your firm entrusts its data with should be recognized by your local state bar or the ABA.

Check your state bar’s print and online publication along with the ABA for information on cloud service providers that may fit your firm’s needs. In addition, technology media and ranking organizations like MSPMentor recognize and rank providers that consistently provide the most reliable and secure cloud service.

When choosing a provider, be sure to verify that they are well-regarded in both the legal and technical communities.

Ensure Your Data Stays Yours (and Stays in the US)

Data Ownership.

It may seem like a reasonable assumption that data you store in the cloud is yours, but don't assume this is the case, even if the provider is well-known and reputable.

In 2012, Google Drive came under fire for claiming the rights to anything a user uploaded, in perpetuity.

If you are using or plan to use a cloud provider make sure that the fine print

includes unambiguous, perpetual ownership of any data you store on their cloud—and ensure that data will always stay within the US. For best results, we recommend using a legal-centric cloud service provider that is familiar with lawyers' ethical obligations and the legal issues around data confidentiality and disclosure.

Data Sovereignty.

One thing every state bar agrees on is that all client and confidential data should be stored within the continental United States. (This applies to cloud-based backups of your on-premise server as well, an area often overlooked by small law firms.)

Surprisingly, the locality of where your data will be stored is ambiguous or simply not defined by many cloud service providers. Microsoft's own Office 365 states that your data may be stored or backed up to countries outside the US. (Just one reason of many to use a cloud

service provider that is legal-centric, and only services the legal industry.) If your firm's data is stored or backed up to a country outside of US legal jurisdiction it will create a whole host of potential ethical issues.



Demand Bank-Grade Security

As we described earlier: The legal industry doesn't have a governmental regulatory body like the financial and healthcare industries. The regulation is from within the profession itself, from ethics boards within profession-regulating associations like State Bars.

The onus is on each practitioner to ensure the IT systems they use, whether they're on-premise or in the cloud, are secure and make every effort protect their client's sensitive data.

Any business, including and especially a law firm, should require that their cloud service provider:

- » Employ 128-bit encryption for all data in transit;
- » Have and maintain enterprise-grade firewalls that perform application-layer intrusion prevention;

- » Employ round-the-clock network security monitoring that watches for attempted or potential security breaches, including failed login attempts;
- » Have strict, documented physical access requirements to their data center;
- » Offers an encrypted/secure email option as part of their email offering;
- » Passes annual SSAE16 audits and posts each annual audit publicly.

Beyond these high-level requirements, ask your current or prospective cloud service provider:

- » What security standard (such as ISO or NIST, as we discussed in Chapter 2) do they employ in their cloud infrastructure?
- » What specific security settings do they enforce in their cloud and of your firm's local, on-premise devices?

What If Your Cloud Provider is Served with a Subpoena?

What happens if you move your applications and data to a private cloud provider's equipment?

And someone serves them with a subpoena?

In our experience, most cloud service providers are woefully unprepared to handle a subpoena. Worse yet, many, especially smaller companies, will panic and hand over your data without even notifying you and giving you an opportunity to fight back.

Read the contract carefully and question the process that occurs in the event of a subpoena of data and records.

Check to make sure your service provider will provide you with adequate notice if records have been requested, or if they receive any request for information pertaining to your firm.

Many cloud service providers, especially those without legal savvy, have no formal process for dealing with a subpoena.



Two-Factor Authentication (2FA) and Restricted Access

Two-Factor Authentication

Most security standards, like the aforementioned NIST, require *Two-Factor Authentication*. With 2FA, users will be required to authenticate by a *second* means before they can log into your firm's cloud environment.

How it works:

- » You log in to an account using your regular username and password;
- » To confirm that it's you, your mobile phone requests confirmation.

This prevents hackers from accessing your accounts because not only would they need access to your username/password combination, but your mobile phone as well.

A security-conscious private cloud provider will offer 2FA, and will accomplish it painlessly with a smartphone app that verifies the authenticity of each user logging into your private cloud.

Restricted Access

One of the primary benefits of cloud computing is the ability to work from anywhere. But what if you don't *want* everyone in your firm being able to log into your cloud from outside of your office?

Make sure your chosen Cloud Service Provider has an option for *Restricted Access*, where you can limit or restrict which staff members can work from home (or elsewhere), and which

firms can only log into your cloud and access your data from within your office.



Onsite Cloud Backup

Presumably you've picked a competent Cloud Service Provider that is diligent about managing backups and keeping their infrastructure up and running.

But even the biggest and best companies can run into problems. And if your data is

lost, your state's ethical board is unlikely to be lenient.

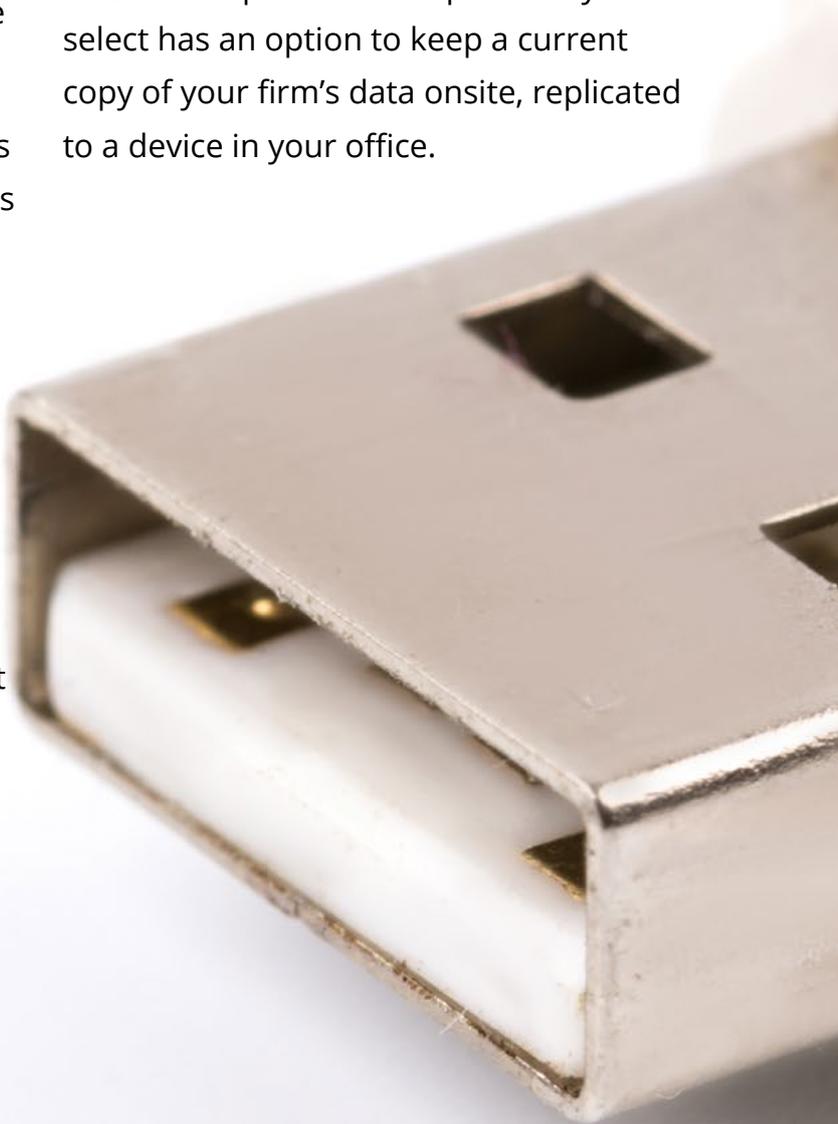
Be sure the private cloud provider you select has an option to keep a current copy of your firm's data onsite, replicated to a device in your office.

Closing the Loop

As with an on-premise server environment, security in the cloud is of critical importance.

This is especially true for law firms, who have an ethical obligation to keep their client's data secure. By moving all or part of your practice to the cloud, your firm is shifting much of this responsibility to your cloud provider.

Make sure they are up to the task.



APPENDIX – RANSOMWARE

We wouldn't be doing an analysis on keeping your law firm secure justice without discussing a rising threat:

Ransomware.

Ransomware is the unholy marriage of computer viruses and electronic theft

How Ransomware Works

Ransomware spreads like a computer virus, primarily by email, as well as certain web sites meant to look familiar, but cleverly impersonated to allow the casual user to unknowingly become infected.

Once the virus infects the computer, it immediately begins encrypting the computer's hard drive and any other attached drives it can find. Any data including documents, videos, images—will be encrypted: forever locked away unless you pay the ransom. We've observed the exact

and fraud. Ransomware is software that spreads like a virus, infects a computer and (without the user's consent) encrypts all of its contents. The victim must pay a ransom to the creator of the ransomware to acquire the key necessary to decrypt their data.

ransom to range from \$200 to \$30,000 USD per incident.

Once the ransomware virus is installed, it will then open a window alerting the user that it has struck, and the only way to decrypt the data is to pay a fee (ransom), which the victim can do right from their computer. See below—a screen shot of a computer infected by ransomware



What Makes Ransomware a Serious Threat

There are a few major factors that make this threat difficult to address.

- » Modern encryption is unbreakable. There is no way to retrieve encrypted data on your own;
- » Lack of Proper Backups. Many small and mid-sized law firms lack the proper backup systems to quickly recover from a ransomware attack;
- » Overseas Perpetrators. Most ransomware schemes are run from overseas, limiting the authority's ability to prevent and stop the organizations and individuals that carry out ransomware attacks;
- » Always Evolving. The actual ransomware viruses are constantly evolving, and commercial virus protection solutions are often a step behind protecting the latest variant.

Ransomware – A Time Bomb for Law Firms

Ransomware is especially damaging to law firms. The servers and computers belonging to law firms often have critical client and case data, time-sensitive and/or deadline-centric data and generally data for which there is a large risk and

penalties if accessed by an unauthorized 3rd party or unavailable to the firm and its staff. Legal filings, scanned documents, images, contracts and more—can all be taken hostage by ransomware.

How to Protect Yourself

Today ransomware is so prevalent, and so difficult to stop—the likelihood of your law firm becoming a victim is relatively high. Here are some measures you can—and should—take to protect your firm.

Managed AntiVirus. Your server and every computer should not only have virus protection software, but the antivirus software should be actively managed by an IT professional or your cloud service provider. That is: someone should be verifying that every device on your network

is protected and the antivirus software is up-to-date. Too often we see small and mid-sized law firms with virus protection systems that are on “auto-pilot”, with no one routinely verifying protection.

Backups. Like virus protection, when it comes to your law firm's backups, it's imperative that you not only have backups, but that a qualified IT professional is managing your backups. Your backups should be reviewed daily, and tested routinely.

Education and Compliance. Most ransomware schemes are run from overseas, limiting the authority's ability to prevent and stop the organizations and individuals that carry out ransomware attacks.

Always Evolving. This is a topic that needs to be incorporated into every law

firm's onboarding process for their attorneys, assistants, and entire legal staff. Require accountability with company rules combined with periodic reviews to ensure awareness and compliance. Focus attention to this important topic, and bring it up in your next all-company meeting, and force password changes at least twice a year.

A Safe Haven in the Cloud

One of the reasons so many law firms are turning to private cloud solutions is the enhanced security and built-in management of their IT platform. With a private, the Cloud Service Provider (CSP) is responsible for protecting their network from external threats like ransomware.

A quality CSP is in the business of providing safe, reliable platforms, and has likely spent the time and resources necessary to protect against the latest cyber-threats. And—since no network can be made perfectly secure—if there is an infection or incident, the onus is on the CSP to react and resolve the infection—not yours.

Closing the Loop

Ransomware is among the fastest-growing threat to your firm's data. Make sure you're properly prepared and protected, and consider a hosted, fully-managed,

secure private cloud solution to take the management and protection of your data off of your shoulders.

MORE INFORMATION

For more information on cybersecurity and cloud computing
for law firms, please contact us:

Uptime Legal Systems
7500 Flying Cloud Drive
Suite 640
Eden Prairie, MN 55344
888-878-4632



info@UptimeLegal.com
<https://UptimeLegal.com>