zola™
media

IT'S ALMOST 2018

Take the Pulse of Your Practice Now...

INTRODUCTION

2017 was one for the records. Whether it was the devastating hurricanes, massive wildfires or online data breaches and hacks, we've all been affected in some way. But for those of us in the legal profession who are ethically obligated to safeguard our clients' most confidential information, the risk of loss is even more critical.

While attacks on major law firms such as Cravath and DLA Piper made the news, the truth is that the smaller law firms are prime targets for malfeasance. Law firms are repositories for social security numbers, bank records, intellectual property and other sensitive information that is highly valuable. Hackers know that as a rule, smaller firms don't have the data security infrastructure and are more likely to pay ransom requests.

This vulnerability is one excuse why some firms justify keeping their data on local servers, or even maintaining hard copies on paper files – which obviously becomes an issue when the office has no power, is inaccessible or … literally under water.

But, there's no escaping the web. Your firm's website and online marketing presence not only gives your prospective clients and referral sources insights into your practice, but also gives clues about your firm's tech savviness and security.

Now is the time to take stock of 2017 and make plans for a better and more secure 2018. To this end, we've put together some tips on how to improve your internal and external security footprint, together with checklists for conducting your own website and legal technology security assessments.

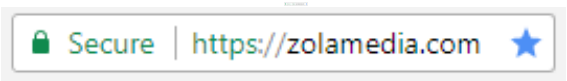
1 WEBSITE SECURITY

IS YOUR WEBSITE MAKING YOU MORE VULNERABLE AND COSTING YOU CLIENTS?

Changes to Google Chrome Will Flag Non-Secure Sites

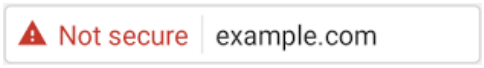
In October 2017, Google updated its popular Chrome browser to add security warnings for website pages that have not obtained a security certificate and collect user data or are viewed in incognito mode. A security certificate is a digital identification that proves that a website has been officially associated with the business or organization represented on the site. It is used in conjunction with SSL/TLS encryption that secures communications between a browser and website user.

Websites that have obtained the certification are designated by a green padlock and the code "https" at the start of the URL.



If your firm's website has not been secured with an SSL certificate, a security warning will now appear on any pages with text inputs, such as contact forms.

This "Not secure" designation will not only prevent you from collecting contact information from prospective clients, but may affect your website's search engine rankings. It will also be a red flag that causes visitors to your site to question whether you have other security protocols in place and resulting in loss of business or worse.



We've put together a website security checklist that outlines the steps you'll need to take to obtain a security certificate and secure your website (**see Legal Technology/Data Security Checklist**).

Confused? Have any questions? **Contact a site security expert at Zola Creative** for complimentary assistance.

2 LEGAL TECHNOLOGY

PROTECT YOUR DATA BY MOVING TO THE CLOUD

Why Cloud-Based Legal Practice Management Software is Safer than On-Site Servers

If your firm has experienced down time due to extreme weather, power outages, viruses or an aging server, you know how frustrating this can be. Nothing is more vexing than receiving a call from a client and feeling powerless that you can't help them because you cannot access their files. Back when the first cloud-based legal practice applications were introduced, there was a fear that storing data in the cloud was risky and could potentially violate a lawyer's ethical duty to maintain confidentiality. Today, the consensus is that cloud-based software applications developed by reputable companies provide more protection and security than on-site solutions.

Impact of Local Conditions Minimized with Enterprise Level Security and Backup

Cloud-based practice management applications such as Zola Suite rely on Amazon Web Services (AWS) to keep your data safe. Documents and data are protected by Identity and Access Management roles within an AWS Region and replicated across Availability Zones (located in different geographic locations within the US) for backup. This means that if one server goes down, the other connecting servers will maintain hosting. With Zola Suite, our external security companies continuously scan for potential vulnerabilities in our applications, systems, and networks and fix them upon notice. Your firm reaps the benefits of the highest security standards at a fraction of the cost.

Other safeguards and advantages built into the application include:

- Hourly backups in multiple locations
- Ability to retrieve data that has been inadvertently (or intentionally) deleted
- Flexibility to restrict access to data on a per-user/per matter basis
- Access on-line anywhere, using any device

ABA Weighs in on Electronic Communications and Data Storage

In May, 2017 The American Bar Association's Standing Committee on Ethics and Professional Responsibility released Formal Opinion 477, which discussed how changes in technology use coincide with Rule 1.6 concerning client confidences. The opinion states that attorneys must exercise "reasonable efforts" to protect confidentiality when communicating via email, storing data on servers or transmitting

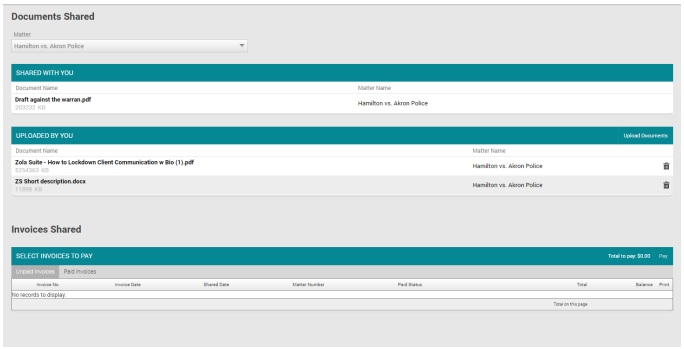
client documents. While "reasonable efforts" are not clearly defined, the Opinion includes these factors as a guideline:

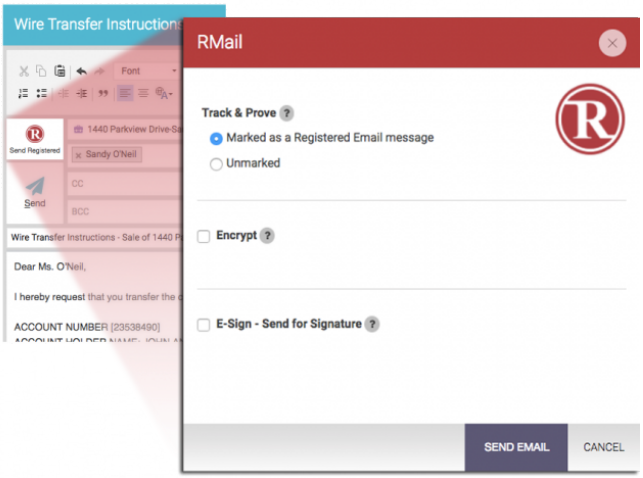
- Sensitivity of information
- Likelihood of disclosure without using additional safeguards
- Cost of employing additional safeguards
- Difficulty of implementing the safeguards; and
- Extent to which safeguards impede the lawyer's ability to represent the client

Cloud-Based Practice Management Software Protects You and Your Clients

Secure Portal for Highly Sensitive Documents: While the full impact of the ABA Opinion isn't clear, comprehensive, cloud-based legal practice software provides law firms with the tools needed to stay in compliance with the guidelines. Regardless of the size or relative tech savviness of your firm, you now have access to secure portals to share sensitive documents with your clients and other third parties. This technology comes with:

- 256-bit bank level encryption
- Dual authentication requiring:
  - Email invitation to join
  - SMS code to unlock
  - Unique password to login
- Ability to grant and revoke access to portal





Built-In Email with Integrated Email Encryption: When the message to be communicated is highly confidential, but more appropriate for email, encryption might be the better way to go. According to a 2015 Legal Tech Survey, only 35% of lawyers use email encryption. Zola Suite is seamlessly integrated with RPost so encrypting sensitive emails sent to clients is just a few clicks away. RPost works with a law firm's existing email address and sends the email message encrypted with no need for additional software or downloads. The Zola/RPost integration also allows a law firm to receive court-admissible proof of delivery.

Ready to move to the cloud? We've put together a legal technology/data security checklist that provides the questions you should ask when assessing legal practice management software (**see Legal Technology/Data Security Checklist**).

Want to learn more? **Contact a practice management consultant at Zola** to schedule a demo of Zola Suite.

Website Security Checklist

☐ Purchase & Install Security Certificate On Your Server

- WHAT IS A SECURITY CERTIFICATE? A security certificate is a digital identification that confirms that your site officially represents your firm or organization. It is used in conjunction with encryption (SSL/TLS) that secures the communications between a browser and website user. Secure websites are highlighted in web browser address bars, generally through a green padlock and the visible "https" at the start of the URL.
- WHERE DO YOU GET IT FROM? While there are a number of providers, you will most likely have to select one that is offered by your website hosting company.

☐ Add Site-Wide Redirects from http to https

- If you enter a URL starting with http://, does your site force a redirect to the secure (https://) version of that URL? If not, you must perform site-wide redirects to direct users to the secure version of your site.

☐ Double Check that All Internal Links Are Relative

- Updating your links ensures visitors and search engines are always viewing your website securely.

☐ Ensure Any External Resources (scripts, images, etc.) are Loading Securely

- In the coding of your site, you may have certain fonts, images or other elements that are being pulled-in via an unsecure link (http://). These links must be updated to the (https://) version of those external elements.
- NOTE: Depending on where those elements are coming from, a secure link might not be available.

☐ Update Your Google Analytics Default URL

- Update the URL in **Google Analytics** by clicking on 'Admin' in the bottom left toolbar and then 'Property Settings.' Under 'Default URL' make sure the dropdown is selected on "https://," add your URL and click Save.

☐ Visit Your Site & Look for the Green Padlock in the Address Bar

- If you do not see a green padlock in the address bar, visit **https://www.whynopadlock.com/** and enter your domain name. This will let you know exactly what elements of your page are not secure.

☐ Optional: Create a Search Console Profile for the Secure Version of Your Site

- Search Console: **Visit Search Console** , click 'Add a Property,' and enter the https version of your website. Click 'Add.'
- Sitemap: Once your profile's been created, you can create a sitemap through the following steps to alert Google that your site is secure:
  - » Click on your new property URL › Sitemap › Add/Test Sitemap › add "sitemap.xml" after your URL into the box.

☐ Test Every Page of Your Website / Review Links & Functionality

- You should see a green padlock on each page and all functionality and styles should be intact.

Confused? Have any questions? Contact a site security expert at Zola Creative for complimentary assistance.

Legal Technology/Data Security Checklist

Questions to Consider When Assessing Practice Management Software

On a scale of 1-10 (1 not at all, 10 extremely), how comfortable are you (and other members of your firm) with technology?

- If you and/or your colleagues are not "tech-savvy", look for software that is easy to learn and configure.

How many professionals (attorneys, paralegals, support staff) require access to data?

- If multiple persons will be using the software, look for features that enhance collaboration and accountability such as task management, work flows and reminders.
- Do you have safeguards in place to ensure that each member of firm only has access to the data necessary to perform their job?

Do you and your colleagues work remotely?

- Can you access critical information when you're not in the office?
- Can you access data from a mobile device?

Which aspects of your business are you hoping to improve through adoption of a legal practice management system?

- Billing & Collections
- Time entry
- Internal productivity reporting
- Calendaring
- Intra-firm collaboration & oversight of cases
- Secure (encrypted) client/opposing counsel communications
- Back up, storage and organization of documents/emails
- Automated workflows

Review, if any, platforms you are currently using for the following:

- Legal Practice Management
- Document Storage/Management
- Backup/Disaster Recovery
- Email
- File Sharing (e.g. Dropbox, Box)
- Hosted Applications (e.g. Office 365)
- Calendar/Docketing
- Time Keeping/Billing
- Accounting Systems
- Project management/workflow
- Other applications

How much are you spending annually on software applications?

ARE YOU INTERESTED IN CONSOLIDATING THESE APPLICATIONS INTO ONE, COMPREHENSIVE, CLOUD-BASED APPLICATION?

Questions to Consider When Assessing Data Security

☐ Are you using cloud-based applications for storing and managing client data?

- The cloud allows you to store and access critical information on a network of servers hosted on the Internet rather than a local server. In case of a disaster, the cloud will deliver a quicker recovery of important information.

☐ Do you use a secure portal to share confidential documents with clients and other third parties?

- Email is not always the most secure means of sharing sensitive information. A client portal will allow your firm to send and receive confidential documents and invoices with people outside of your firm without the risk of third party interceptions.

☐ How frequently do you backup your data?

- Regularly backing up your clients' confidential information should be a part of your firm's daily routine. Backing up your data weekly on a Sunday night could cause a problem if your server crashes on a Saturday. Cloud-based practice management software applications are designed to backup data hourly, 365 days a year.

☐ Can you monitor firm-wide activity relating to matters to prevent security breaches?

- Technology that provides an uneditable, firm feed that keeps you apprised of all matter-related activities will point out when something just doesn't seem right.

☐ Do you know when and how to send encrypted emails?

- Encrypted emails should always be sent when the content contains privileged or highly sensitive information if it were to be intercepted by a third party. Send such emails using an email encryption service, such as RPost.

☐ Is your data stored in state of the art, highly secured data center with network firewalls and multiple locations?

- Most small law firms do not have the technical or financial resources to employ sophisticated security measures with multiple redundant backups. Reputable legal technology companies that utilize Amazon Web Services (AWS) or other leading cloud companies benefit from infrastructures designed to meet the requirements of the most security conscious enterprises.

☐ Is your mobile application secure?

- When storing client information on your mobile app, make sure that you use touch ID authentication so that if your phone is lost or stolen, this information cannot be accessed by anyone else.

☐ Do you utilize court-admissible proof of delivery, time and email contents?

- It is not accurate to assume that an email was delivered because you didn't receive a bounce back. With registered email technology, you can view a delivery audit trail and remain sure that your information was received by the intended party.

Want to learn more? **Contact a practice management consultant at Zola** to schedule a demo of Zola Suite.