**PANIC**

[YOU NEED A BETTER PLAN]

FOR DATA BREACH PREVENTION AND RECOVERY

Attorneys are often exposed to risk simply because they do not possess a data breach response plan.

Data Security: Preventing Breaches and Planning for Recovery

Attorneys and law firms are often exposed to risk merely because they do not possess a data breach response plan. Those who have taken steps to prevent the occurrence of a breach and have prepared in the event one should occur will survive and suffer less damage.

9

VIRTUAL IMPRESSION
YouTube Remarketing

Remarketing offers law firms an opportunity to recapture the elusive attention of website visitors who fail to convert to clients the first time around. Think of it as your second chance to appeal to your best prospective clients.

3

MESSAGING
Online Reviews Matter

Online reviews are an important part of a law firm's marketing strategy. But attorneys may be reluctant to ask for reviews out of fear that these critiques will not reflect the message the firm wants to convey.

15

DESIGN
OBITER DICTA

What do the best attorney websites have in common? Here are five key items.

Ask 20 people what is best about a website's design and you will likely receive 20 different answers. A good website, however, is one that delivers traffic and conversions. Ideally, a good website is also visually striking, with attractive design that goes hand-in-hand with performance. But not always.

Designing a website that holds visitors' attention and convinces them to take action is a balance between listening to what users say they want and subtly pushing them to do what you want. To achieve that balance, your site should proactively answer your visitors' questions, while providing reasons to contact you.

One item that makes almost every list of "top things an attorney website should have" is a responsive layout. This item is not included on this version of *BLF*'s official list because it is, at this point, essential to all sites. Google lists its responsive web design articles in the "Web Fundamentals" section of its developer site, and mobile-friendliness has been an officially announced ranking factor for over a year. All websites should be responsive or have a dedicated mobile layout.

1. Clear contact information
For the purposes of conversion, your phone number should be on every page of your website, and for the purposes of local SEO, your address should, too. Your mobile site should display a clickable phone number prominently so that visitors can easily tap to call you. Links to additional information, like appointment forms, other office locations or office hours must be easy to find. You may also want to consider adding supplemental contact avenues, like an online chat. Be sure any forms you use to collect initial contact information are brief. The likelihood of a user finishing and submitting a form decreases with every input field.

Bottom line: Make contacting you easy, but do not force it. Too many pop-ups or over-the-top calls to action will turn visitors off.

2. Good attorney bios
Attorney bio pages are some of the most visited pages on a law firm website. Yet, they receive little attention. Many attorney bios are painfully boring and written with language so stilted that it is difficult to image the person behind the bio. Your attorney bio page is not your resume. Yes, you should include some basic information about

education and experience, but beyond that you must talk to clients. Clients care how you can relate to them and solve their problems. Tell them what they can expect from working with you and why you are passionate about your practice areas. Include personal anecdotes. In short, be authentic and approachable.

3. Social Proof
Social proof includes reviews, testimonials and client videos, if available. Currently, 92 percent of consumers read online reviews, and 88 percent trust reviews as much as personal recommendations. And this trend is growing. Over 50 percent of people aged 18 to 34 report trusting online reviews more than opinions of friends and family. If you are avoiding using reviews, you are missing a valuable conversion opportunity.

4. Humanity
Attorneys often hesitate to show too much personality for fear of seeming unprofessional. Strangely, this appears to be exclusively an online phenomenon. When meeting clients personally, attorneys do not use legalese; they connect on a human level. Try doing the same with your website. Incorporate natural, unposed photography and write content that displays empathy and understanding of client issues.

5. No generic filler
There is no excuse for using uninspiring content and generic photography on your website. You do not need to display images of gavels, courtrooms or the American flag. Your visitors understand they are dealing with the U.S. legal system. People who are searching for an attorney online are also looking for in-depth information about the law. Take the time to write helpful practice area pages. Offer case studies, or, if you cannot talk about your cases, present example scenarios. Invest in custom photography. Treating your visitors with respect will bring its own reward.

- Kristen Friend

YouTube Remarketing
a second chance to make a lasting impression

Remarketing offers law firms an opportunity to recapture the elusive attention of website visitors who fail to convert to clients the first time around. Think of it as your second chance to appeal to your target audience.

Getting people to your website is just the first step. Once visitors land on the site, they must be persuaded to stay and look around. The ultimate goal is for them to take action by contacting you. However, the decision to hire an attorney is rarely immediate. A website visitor may be researching lawyers in order to make a decision in the future. Or, the visitor may get distracted by a phone call or other websites competing for attention. Such visitors may still be valuable leads.

Remarketing campaigns allow law firms to reach out to potential clients who have left their websites undecided and those who may not be prepared to hire a lawyer but who will need one in the future. The key idea behind remarketing is that the best prospective client is one who has previously expressed interest in your services. Research indicates people who have engaged with a brand's content are more likely to convert into clients than first-time visitors.

Remarketing is a pay-per-click product, so fees only apply when an ad is clicked. The targeted approach is cost-effective, encourages visitor engagement, results in improved brand recall, maximizes marketing ROI and yields higher conversion rates than other types of paid ads.

Remarketing is an AdWords product that uses the Google Display Network, which reaches 90 percent of internet users worldwide. Most people have experienced remarketing in the form of being followed by an ad from a site they visited. Remarketing uses cookies, or small chunks of data. When a visitor meets a set of predefined criteria — such as accessing a particular page or clicking on a certain link — a cookie is stored in their browser. After leaving, they will continue seeing either text or banner ads on other sites.

You can add people to your remarketing list anytime they land on your site. Lists can be segmented to specifically target an audience. For instance, if visitors spends time on your car accidents page, they can be shown ads that are related to that practice area. Attorneys can display different ads to visitors who fill out a particular form versus those who visit the website's About page. The technique ensures your firm never ventures far from the potential client's mind.

Video is currently one of the most popular formats for user engagement and information sharing. According to Cisco, global video traffic will comprise 82 percent of all consumer internet traffic in 2020. Attorneys can take advantage of this trend by using YouTube remarketing. With its more than one billion users, YouTube has proven to be a consistently dominant force when it comes to online video reach.

Although remarketing traditionally takes the form of text and banner ads, the video format provides law firms with another opportunity to directly convince potential clients to hire them. Attorneys can display targeted ads to viewers across YouTube and video partner sites.

YouTube remarketing works on the basis of viewers engaging with video content as well as visiting your website. When an individual watches video content on a YouTube channel, they can be identified by a unique cookie. These individuals can then be targeted when they watch videos on other sites. When users click on video ads, they revisit the firm's website with a greater potential of being converted into actual clients.

The simplest way to start a YouTube remarketing campaign is with an existing Google AdWords account. When an individual performs a certain action, that information can be saved to a remarketing list. The remarketing lists can then be selected for a new video ad or an existing video campaign. Creating targeted lists and campaigns ensures that video content reaches users who have engaged with your past content based on your selected criteria.

There are numerous benefits to YouTube remarketing. First, it is cost-effective. Because your video ad is reaching the potential clients on your remarketing lists, it is likely to generate more conversions for the marketing budget allocated to video advertising. In addition, videos enable lawyers to connect more directly with viewers in comparison to conventional image and text ads. Videos provide the opportunity to build a relationship with your prospective clients in a way that is unique from other platforms. The ultimate goal is to capture the viewers' attention and explain how they can benefit from your law firm's services.

YouTube video advertisements take the form of sponsored related videos or pre-roll ads, also known as in-stream video ads. The latter generally ranges from 15 to 60 seconds in length. Pre-roll ads are inserted at the beginning of videos. Such ads provide exposure while saving money; the only time you pay is if someone watches the video ad for 30 seconds or more.

Online video advertising achieves the best results and maximum impact with the combination of quality visuals, proper targeting and sufficient reach. Bearing in mind that users have short attention spans coupled with the ability to skip video ads, in many cases, it is essential to convey your message within the first five seconds of the video.

Creating a polished, high-quality video requires a crew, proper sound and lighting, and a person with good on-camera presence. Attorneys who are reluctant to invest a hefty chunk of their marketing budget on producing expensive, original video content or video ads have the option of using VideoScribe. The app allows users to create and customize whiteboard-style animation videos. It is easy to use and often more viable than traditional video.

Some businesses may be reluctant to use remarketing because of the perception that users may feel irritated or uncomfortable with constantly being followed around the internet by ads. However, studies indicate remarketing campaigns result in higher conversion rates over time. In addition, filters offer the option of choosing how long a cookie ID should remain on a marketing list. Therefore, law firms can prevent users from continuously seeing the same ad over and over again.

Lawyers can generate real engagement and results from their YouTube efforts by turning their focus to remarketing campaigns as an effective strategy for pursuing conversions. By combining video advertising with remarketing, law firms will be able to reach valuable leads with a greater likelihood of converting potential clients. Think of YouTube remarketing as your brand's elevator pitch. What would you say if you had an uninterrupted moment with a potential client?

- Dipal Parmar

*video*TIP

A remarketing list can be created by linking a YouTube account to an AdWords account. Linking both accounts helps you choose specific videos for remarketing. After linking the accounts, video remarketing lists can be created to target people who have taken the following actions:

• Viewed any of your videos on any network or website
• Visited or subscribed to your YouTube channel
• Interacted with your videos by sharing, liking or commenting
• Viewed your video as an in-stream video ad, also known as a pre-roll ad
• Visited any page on your website

LESS EMAIL, MORE COMMUNICATION
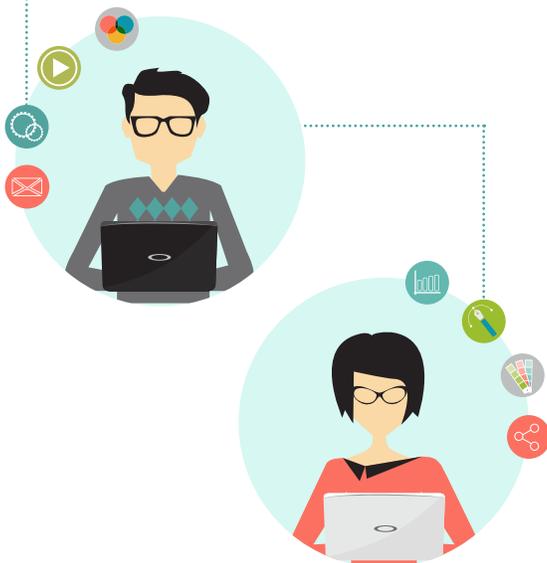
The market for collaborative software is relatively young, but expanding rapidly. Several leading products are low-cost, feature-rich and stable enough for daily use. The feature sets across products tend to be similar, yet they are fluid enough to make a comparison in terms of accuracy.

Email is increasingly a frustrating matter in modern business. Ten years ago, the majority of email you received was from another person – it was usually something you genuinely wanted or needed to read. Now, the majority comes from machines: marketing, mailing lists, financial statements, social media notifications and the like. At larger organizations, even the email that comes from individuals is often a nuisance. Getting cc'd on a host of emails that are slightly relevant to one's work is a constant frustration for many, but is often viewed as a necessity. You may hesitate to open your email in the morning because of the difficulty of sorting the important messages from the rest.

Enter "collaborative software." At its root, collaborative software is a communication tool. It is a replacement for email and instant messages. It handles files, just as you can attach files to emails. And it aggregates communication by topic, project, work role or social proximity – just as email threads and instant message groups do.

Collaborative software platforms like Slack and Glip, can be worthy of consideration and testing. Slack is a leader in the space, while Glip is a somewhat smaller competitor. Other popular products include HipChat, SamePage, Bitrix24 and eXo Platform.

The basic structure of most collaborative software is a three-pane window not unlike many email programs. The left pane contains a list of people in your organization with whom you can communicate one-on-one. It also contains a list of "channels" (a.k.a. groups, teams, etc.), each of which pertains to a particular topic and comprises some number of team members. Clicking on an individual or a channel fills the center pane with a persistent history of the communication that has occurred there. The right pane contains a list of files and links that channel members have contributed to the conversation. The details change between software products, but this is a common layout.

Collaborative software is intended to reduce our need for email and instant messaging, but so far, it may sound a lot like email and instant messaging. So why are thousands of organizations adopting these products?

Advantages of Collaborative Software

All communication on a topic is grouped together

Say you need to refer to information that was emailed to you in the past. Just think how difficult it can be to effectively search your email. Who gave you this information? How long ago? What was the subject line of the email? What keywords did they use to convey the information? Was it an email, or was it an instant message? Or maybe a text message?

If you use collaborative software you know what channel all information resides in, regardless of who sent it. There is no email, instant messages or text messages to consider. All you need to figure out is how far back to look. Searching a channel for a keyword is easy, and so is scanning visually for context, because all communication happens in one stream.

Catching up someone new is easy

Imagine you bring a new associate or staff member into your firm and you need to get them up to speed on a case. A lot of important detail is probably spread out among many email threads.

You might forward all of those email threads to the new person and hope that they can make sense of it all. For you, that means searching through your email, and for the new employee, it means a lot of time spent trying to understand the context of different threads that may overlap in time as well as content. Going forward, everybody needs to remember to copy the new

team member on each relevant email. With a collaborative tool, all communication regarding a specific client or topic happens in one place. Once you give a new team member access, they immediately have access to all past and future communication on that matter. The most recent communication is at the top of the feed; the most important messages and files are pinned for easy reference; and the user can decide for themselves how far back to read for their own purposes.

Wrangling internal email and enhancing communication

Collaborative software can serve to enhance two types of communication at law firms: internal and client-directed.

Internal communication occurs between attorneys, paralegals, and staff at the firm. It could also include co-counsel or vendors with whom the firm has close relationships. This is where collaborative software excels. Any small to medium firm can expect to eliminate the vast majority of internal emails in one fell swoop upon adopting collaborative software. If you make a concerted effort to communicate the importance of the switch and get everyone to sign up and install the software, you should immediately find that it obviates virtually all internal email — which obviously helps you keep your email inbox under control.

Client communication

In most industries, external communication with third parties is still primarily the domain of email. However, this is where law firms have a unique advantage in the nature of their relationships with clients. As an attorney, you are largely free to decide upon any reasonable method of communication with your clients. If you suggest that collaborative software is the way to go, you probably will not receive any push-back – and particularly not from young or tech-savvy clients.

> **COLLABORATIVE SOFTWARE CAN ENHANCE INTERNAL COMMUNICATION.**
>
> -
>
> *Collaborative software allows you to maintain separate channels for the discussion of discrete topics. This serves much the same purpose as email threads, but presents the information in a more user-friendly and appealing way.*

Both Slack and Glip allow you to invite third parties (e.g. clients, contractors, and vendors) to join one or more channels. You can spare the client the daily chatter and details that might worry them unnecessarily by creating two channels for each client or topic: one for internal communication and a second for communicating with the client. All firm staff would likely be members of both groups, but the client would only be invited to join the latter.

The client would get regular updates and see that all applicable attorneys and staff members are available for communication, but would not be bothered with early drafts of important documents.

Many practice management software products offer "client portals." These are private, online spaces where attorneys and clients can communicate and share files. These work similarly to collaborative software, and if you have used one, you are probably already a fan. Client portals are a great feature, and they can complement a collaboration solution.

COLLABORATIVE SOFTWARE IS...

Integrated with other services you may already use. Linking with services like Google Drive and Dropbox streamlines the workflow as you move between the different sites and services your firm uses.

Cloud-based and secure. The security and redundancy offered by any well-funded cloud software company is stronger than what you can achieve on your own. The weakest link is your password. Use a unique, non-dictionary password at least 12 characters long, and consider changing it on a regular basis, perhaps twice per year.

Cross-platform. You can access your work from any web browser. Installable apps for your computer and smartphone are available for all major platforms.

Inexpensive. A free initial trial is very common, and some products offer a free monthly plan that may suffice for small teams with limited needs. Even medium-size firms should find the software quite affordable.

Customizable in its notifications. Desktop and mobile notifications are customizable so that you can decide which channels you always need to stay abreast of and which can wait for you to catch up when you get time.

Are there downsides?

Collaborative software is a new trend. Inevitably, some of the players in the space will go under. If that happens to the one you use, this will at best mean an interruption in your productive work while you seek an alternative solution. At worst, it could theoretically mean your data is inaccessible. As unlikely as this is, it is important to understand that it is possible.

Most products allow you to export all your data to downloadable files. As you test out a tool for use at your firm, go through the export process. It is simple, and you should understand how to use the resulting data in the event the service is inaccessible.

The learning curve involved with any new software is clearly a downside compared with maintaining the status quo. However, most people who are comfortable with modern online software should have no trouble getting started and will likely find the entire process highly intuitive. If you do not, you should probably try another product.

Recommendations

Read some current reviews and recommendations for collaborative software online. Be sure the information is recent, as these products' feature sets change regularly. Make a selection based on your own criteria, whether the cost is dependent on your anticipated usage, the specific features available, or simply the look and feel of the service and site.

Download and install both the desktop and mobile software for each product you are considering, and have at least one more person at the firm do the same. This direct comparison and shared experience will elucidate minor advantages and disadvantages that might otherwise go unnoticed.

When you have decided which software fits your firm best, explain to each team member the importance of having everyone on board. Internal communication, which is not one-on-one, should move to the collaboration solution immediately and completely. This way all ongoing conversation on any given topic can be found just where it is expected.

Even if the appeal of collaborative software can be difficult to grasp for those who have not used it, thousands of companies across many industries have made the move. If communication at your firm could use an upgrade, give it a try. The only thing you have to lose is thousands of emails.

- Ryan Conley
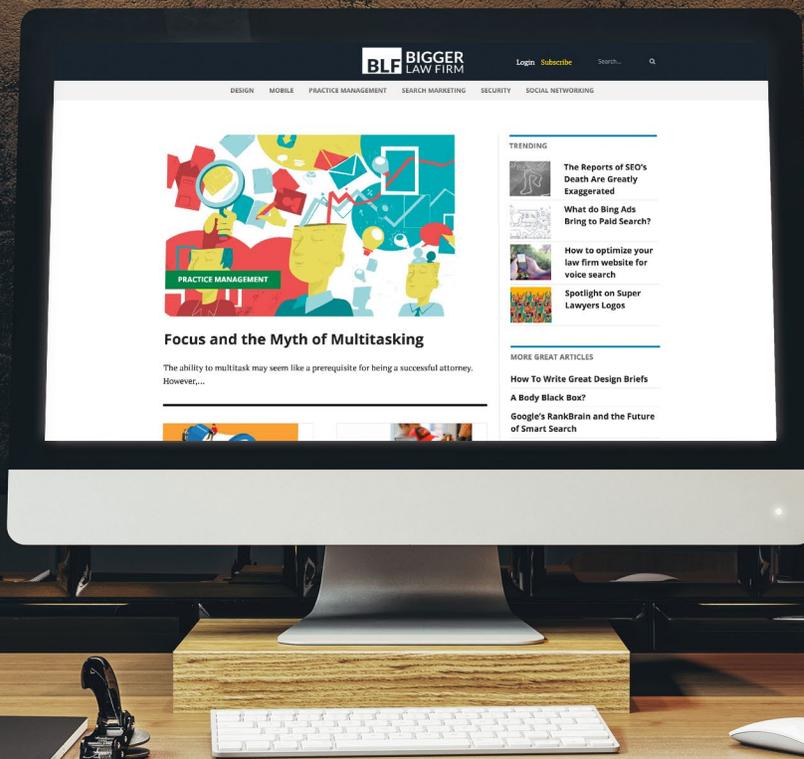
YOU NEED A BETTER PLAN

for data breach prevention and recovery

Data breaches are becoming too common. According to the FBI, hundreds of law firms have fallen victim to data breaches committed by hackers. Data breaches range from theft or loss of laptops or mobile devices to interference with a law firm's network, containing files one year or older.

Attorneys have an ethical duty to take reasonable steps to protect information relevant to their clients. They also have an ethical duty to inform clients if there has been a breach of client data. In order to be in compliance with these duties, attorneys must establish information security programs, IRPs. Those who have taken steps to prevent a breach and have prepared in the event one should occur will survive and suffer less damage.

Maintaining data security

In the past, the focus of law firm security was on preventing cybercriminals and hackers from infiltrating firms' data. Initially, firms installed anti-virus software, ranging from the very basic to the more advanced, and then anti-malware security suites, next-generation security appliances and other technical defenses.

However, even as there have been technological advances in the various types of defensive software, would-be hackers have grown more adept at accessing data. As a result, detect and respond is the new catchphrase in cybersecurity. Although detection and incident response have been essential aspects of information security for years, they are now not nearly as important as protection. According to Gartner, a premier technical consulting firm, by 2020, 75 percent of all businesses' information security will be earmarked for detect and respond methods. This represents an increase from less than ten percent in 2012.

Identify, protect, detect, respond and recover

Identify, protect, detect, respond and recover is the principal aspect of the National Institute of Standards and Technology's Framework for Improving Infrastructure Cybersecurity Version 1.0, issued in February 2014. The objective of the framework is to provide security of critical infrastructure, and realize improvements in cybersecurity programs.

While "identify and protect" applies to the beginning stages of cybersecurity, "detect, respond and recover" have emerged as the new focal point in security from breaches. It can be particularly challenging if you are unaware that you have suffered a security breach. The typical victim has been breached for seven months or longer prior to the discovery of the breach.

> Attorneys are often exposed to risk simply because they do not possess a data breach response plan.

The Incident Response Plan

Advance planning is key to getting ahead of any threat, which consists of a procedure referred to as an Incident Response Plan (IRP). An IRP is frequently directed toward data breaches. Some examples of incidents these plans provide a response to include: ransomware, resisting attempted hacks, access of data by an insider without permission, or dealing with the theft or loss of a laptop or mobile device. While the majority of large law firms

A law firm's team may consist of all or any of the following categories: management, IT, compliance, information security, marketing, human resources and any other departments. In the event a breach occurs at night or on a weekend, it is important to set up a conference call bridge line. The plan should contain contact information, including home and cell phone numbers and personal and work email addresses. The list will have to be updated on a regular basis as people join or leave the firm.

Refrain from speaking too quickly prior to an investigation into the circumstances surrounding a data breach. A common error is attempting to lessen the harm, but really expanding it as the extent of the breach is different than what you initially thought.

have implemented such plans, many smaller firms have not. Increasingly, clients and insurance companies are requesting to conduct a review of law firms' IRPs. Due to the rising prevalence of data breaches, now is an opportune time to establish and carry out a plan or revise an existing one so that it is up-to-date.

It is best not to use a template IRP. While you can start with a template, be aware that no two law firms are exactly the same, and each has a different business process, network infrastructure and data. An IRP should be tailored to suit the firm. The size of the plan is likely to correspond to the size of the firm.

Components of an incident response plan

It is recommended that law firms identify the functions mentioned in the IRP by the titles of the positions, and not by an individuals' name, because people may leave for other positions.

1. Hire a data breach attorney

It is recommended that law firms secure the contact information for a seasoned data breach attorney. Several large firms currently contain departments that emphasize security and data breach response, while some smaller firms are directing attention to this area. It would be unwise to think that you can manage security and data breach response without the help of an attorney who is versed in data breaches. Under the attorney-client privilege, the data breach attorney may be able to safeguard a large amount of information relevant to the breach investigation.

Moreover, make sure that you know where to find your insurance policy, which should provide coverage for data breaches. Make certain that you have coverage, and are in possession of the insurer's contact information because you will have to call your insurer immediately should you become aware of even a potential breach of security.

2. Contact law enforcement

It is a good idea to have the contact information for law enforcement, such as the FBI, who are frequently the first people who are contacted in data breach cases. Additionally, secure the contact information for the digital forensics consultant you would like to have conduct an investigation into the cause of the breach, and provide a remedy.

3. Contain and recover

It is recommended that the IRP includes a section on containment and recovery from a breach. A law firm that has suffered a breach is at a greater risk of being subjected to a breach again, or having a continuous breach. This could be because the breach has not been completely controlled, or because the hacker has uncovered areas in which the law firm is not fully protected and that can be manipulated at a future date.

Find out what data has been compromised, or potentially compromised. Also, determine whether all data was encrypted while it was being sent or stored. If it was, then this may diminish the burden of notification. You should also recognize any PII, personally identifiable information, or information that could have been compromised.

4. Preserve information systems

Identify and safeguard the systems logs with respect to your information systems. Be sure to turn on logging functions and retain logs prior to the occurrence of any breach. If you are in possession of intrusion detection or data loss prevention software, record all system logs from the software and give them to your investigator. If you do not have any such software, you may wish to consider acquiring it in order to secure the data for your law firm. In the event your bank authorization has been compromised, obtain the contact information for your bank.

5. Employ a public relations firm

Although it is not required, it may be to your advantage to find a reputable public relations firm. If you do not have to publicize the breach, you may not have a need for such a firm. However, if the breach is made public, you may have to engage in some immediate damage control. You may be able to obtain coverage for this through your insurance company. If so, then your insurance company will refer you to a suitable firm.

6. Disclose the breach to clients

Be advised that it may be challenging to handle clients and third parties in such a way that you do not disclose everything and yet maintain some semblance of transparency. It is important to exercise caution when planning to inform clients of a breach. This is because a data breach that has been publicized could lead to a large departure of clients from your firm.

Refrain from speaking too quickly prior to an investigation into the facts and circumstances surrounding a data breach. A common error is attempting to lessen the harm, but really expanding it as the extent of the breach is different than what you initially thought.

7. Notify employees

Think carefully about how you will notify your employees about any data breaches. Make sure that the law firm communicates with a single voice, and that employees do not circulate information about the breach. Decide whether to share information about the breach on social media, and, if your will be doing so, devise a plan to reveal such information in a manner that will cause the least amount of damage to your firm.

8. Test the plan

Test the plan by having a rapid walk-through of possible scenarios,

Law firms should prepare for the time at which they will fall victim to a data breach, and not for the possibility that there will be a breach.

after which you can conduct a complete exercise of the plan. Incorporate contacts with outside resources to make certain that everything is updated. This will assist in familiarizing everyone with the plan and in recognizing areas that need improvement.

Breach notification law

If your state has a breach notification law, and nearly all do, write it in the incident response plan, along with the rules of compliance. You may have to consult your state Attorney General. Because laws governing breach notification are very different, you should be knowledgeable about the law in your state. In addition, identity whether other states' breach notice laws are applicable. They could apply to the residences of employees or clients, or remote offices.

Make certain that all pertinent data breach laws are mentioned in the plan, and are appended to it. Recognize any affected data that is subject to other legal obligations such as HIPAA or specifications within client contracts, and compliance with notice demands.

Determine whether the prospect of a breach requires the revision of IT

and information security controls and policies. On the basis of what you gleaned from the test, also decide whether the incident response plan should be modified. The plan should state that an annual review is mandatory, even when there is no occurrence of a breach.

Preparation is key

Law firms should prepare for the time at which they will fall victim to a data breach, and not for the possibility that there will be a breach. In order to be ready for such an eventuality, they must implement security programs that consist of detection, response and recovery, and recognition and safeguarding of data and information assets. An effective incident response plan is necessary to achieve a favorable result.

Attorneys who have taken steps to prepare for a breach are more inclined to survive and experience less harm. However, those who do not sufficiently prepare will likely expend more funds, waste more time, and endure an increasing number of difficulties with clients and public relations.

- Roxanne Minott

Local Schema Address Markup
Are top ranking websites using it?

Structured data allows authors to articulate exactly what their content means to search engines.

Organization of information on web pages and throughout a website is the key to good results. A well-structured website with clearly organized code helps both visitors and search engines navigate through pages, enhancing user experience and Google's ability to rank page content. Structured data enhances search engines' ability to understand exactly what is on your pages and how it should be prioritized.

When you implement structured data into your content, you qualify for two features of Google Search: Knowledge Graph and Rich Cards. Knowledge Graph is an intelligence-based technology used by Google. When your website is considered a leading authority for a subject matter, Google will deem your structured data as credible and use it as an answer throughout Search and other Google-owned properties. Rich Cards is a format designed for improved mobile experience. Rich Cards puts an emphasis on visual display, such as displaying an image along with a recipe on mobile search. Rich Cards is an evolution of Rich Snippets, which are used to display certain information within listings on results pages.

Introduction to Schema.org

On June 2, 2011, America and Russia's largest search engines: Google, Bing, Yahoo and Yandex respectively, came together to collaborate and create a unified set of schemas for data comprehension. The result of this collaboration is published at schema.org.

A schema is a template or blueprint of how a database is constructed. Along with the vocabulary in schema.org, MicroData, RDFa, JSON-LD and other formats used to understand data, are included. Google recommends using JSON-LD for your markups. These search engine giants hope this partnership will promote organization on the internet.

You do not need to understand all of the technical aspects of schema, only its results. Schema information tells search engines the meaning of certain information, like the time and date of an event or the aggregate rating of an article. Most pieces of data have the potential to be marked up with some type of identifier.

Schema PostalAddress, a comparison

```
<h1>Beachwalk Beachwear & Giftware</h1>
A superb collection of fine gifts and clothing to accent your stay in Mexico Beach.
3102 Highway 98
Mexico Beach, FL
Phone: 850-648-4200

--

<div itemscope itemtype="http://schema.org/LocalBusiness">
<h1><span itemprop="name">Beachwalk Beachwear & Giftware</span></h1>
<span itemprop="description"> A superb collection of fine gifts and clothing
to accent your stay in Mexico Beach.</span>
<div itemprop="address" itemscope itemtype="http://schema.org/PostalAddress">
<span itemprop="streetAddress">3102 Highway 98</span>
<span itemprop="addressLocality">Mexico Beach</span>,
<span itemprop="addressRegion">FL</span>
</div>
Phone: <span itemprop="telephone">850-648-4200</span></div>
```

How schema markup can benefit SEO
A search engine determines a website's value by how informative and receptive it is to consumers. Schema markups allow web crawlers, bots that browse and index content on the internet, to effortlessly deduce data. This in turn improves user experience and results in a search engine favoring your website.

In order to stand out, most advertisers use a rich snippet. A rich snippet is extra text generally found under a search listing. It could be extra information pertaining to your services or product. A Searchmetrics study in 2014 showed 36.6 percent of Google searches supported schema rich snippets, yet only 0.3 percent of websites are using it. Being in the extreme minority of websites that utilize this tool will help your listing look more attractive to users, possibly increasing your click-through rate and achieving greater conversions.

Why law firms should use schema PostalAddress
Schema PostalAddress is a specific schema markup vocabulary used to better decipher local businesses' location information. As a local law firm, it is critical your address is presented in a way that both the user and a web crawler can easily comprehend.

At the top of the page is an example of a local business's address and description both with and without schema PostalAddress markup. A person will be able to discern the information without markup, but a web crawler might not be able to. We know, because of the way the information is structured, that Beachwalk is the name of the store. A web crawler, however, could mistakenly assume that this is an available activity, along with beach apparel and gifts for sale. With markup, the bot will know which text is the business name, street address, city and region. You cannot afford to risk your brand being mislabeled or misinterpreted.

BLF experimented with Google to see how many top ranking law firm websites use schema PostalAddress. We chose thirteen cities, with some of the highest populations in the country, and competitive practice area keywords such as personal injury or estate planning. Of the 188 law firms *BLF* surveyed, 93 or 49 percent of law firms on the local map used schema PostalAddress markup and 144 or 76 percent used some form of schema markup. This indicates that using schema markups may be a minor ranking factor.

How to implement schema markup
The process of installing schema markups to your website may be tedious as you will need to make the changes for individual pages, but it is overall a straightforward procedure. It will also be rewarding for you in the long run.

First, go to Google's Structured Data Markup Helper. Select the nature of the content to markup, such as software application or local business. Enter the URL you wish to markup, then highlight the specific text, and select the distinct markup you want it to correspond to. Continue with this method until you are satisfied with the content being marked, then click Create HTML.

If you are comfortable editing template files and code, you can do the following manually; otherwise it is recommended to let your webmaster make the necessary updates. Download the generated HTML file and add the highlighted relevant snippets to the appropriate areas of your CMS or source code. You can also do the action from the View HTML tab of the page. When completed, click Finish.

Use Google's Structured Data Testing Tool to evaluate whether you performed the changes correctly. You can either enter the URL of the page you just edited or the code snippet. Whichever option you choose, you will be able to see whether the tool can detect the markup within the text.

Markup as much visible content as possible. The more you do, the clearer your data will be for web crawlers.

Schema markup is a form of search engine optimization and innovation destined for longevity. When the country's largest search engines band together for a collaborative effort, it shows how important they believe schema markup is to the future of search. Implementing it onto your website will allow you to stay on track toward what Google's mission statement has always been: making information accessible.

- Dexter Tam

ONLINE REVIEWS MATTER

Online reviews are an important part of a law firm's marketing strategy. But attorneys may be reluctant to ask for reviews out of fear that these critiques will not reflect the message the firm wants to convey.

While you cannot control what clients write, it is imperative that your firm take an active role in incorporating online reviews into your marketing plan.

Raw firms cannot afford to ignore online reviews, because prospective clients use them in searching for an attorney and making their decision about which firms to contact. A large and growing percentage of clients use online search engines to find an attorney, but it is important to note what they do next after hitting the search button. Google Consumer Surveys asked consumers this question, about searching for a specialty lawyer on Google, with 27.6 percent responding that they would read the reviews on Google and 18.4 percent saying they would read reviews elsewhere on the Internet. Another 29.5 percent said the first thing they would do is visit the lawyer's website.

One of the most important factors that has increased the importance of online reviews is the fact that Google automatically includes them as part of search results.

Some prospective clients may set out with the idea that reading online reviews is an important part of choosing a lawyer, and they may click on Avvo or Yelp to do so. But a firm's Google rating is part of Google search results, whether the user is seeking out reviews or not. A law firm needs to be near the top of search engine results pages, and clients need to have a reason to click. A low rating, or no rating at all, simply will not do.

People are already reviewing your firm

The legal profession has long had a complicated attitude toward advertising, with many attorneys feeling that building one's reputation through word of mouth is a superior way to gain business. As law firms have adapted to the Internet era, any squeamishness about online legal marketing has largely fallen away. That said, the distinction between a crass advertisement and a sophisticated marketing strategy remains paramount.

Online reviews are the perfect union of our modern online world and the traditional notion that an attorney's reputation should be built on word of mouth. Internet reviews are the online manifestation of a law firm's reputation, and they should command the firm's attention.

Reputations are powerful because what other people say about a firm – or any business – is thought to be more objective than what a firm says about itself. As online reviews become more popular, there is no way for law firms to opt out. Clients are already posting reviews of attorneys on a number of different websites, and reportedly more people are inspired to speak out when they are dissatisfied than when they are satisfied. That is why law firms need to take a forward-thinking approach to influence the conversation.

How to handle negative reviews

Many law firms have ignored the issue of online reviews until a negative critique made them sit up and take notice. Often the first response is, "Can we get that taken down?" Usually the answer is no, but it should be noted that reviews containing false allegations may be actionable as defamation, and some attorneys have had success fighting outrageously false reviews in court. However, before taking such a step, consider the Streisand effect. A legal battle over a negative review may bring more attention than the original criticism itself, so you should make sure the resulting publicity will not reflect poorly on the firm.

Defamation aside, the vast majority of negative reviews are statements of the person's opinion posted on a third party website, so the law firm has no control over what is posted. Generally,

what a firm can do is limited to two things: respond to the negative review in a professional manner, and drown out the criticism with accolades.

There is some debate over whether or not law firms should respond to a negative review, with some arguing that they should be ignored, to avoid calling more attention to them. This may be the case if someone posts a one-star review with no explanation. Such a review contains no real information and will be counteracted by the many positive reviews the firm will solicit.

However, if a review contains a substantive and potentially damaging critique, a professional response may be appropriate. Caution is advised, for several reasons. First, the firm must not reveal any confidential information about a client's case when responding to their review. The firm should also not encourage any more of a public dialogue with the dissatisfied client.

Keep in mind that the real audience for the response is not the person complaining, but any other potential clients who may be reading. The firm may wish to state in its response that it cannot respond to specifics about a client's case, as confidentiality must be protected. The response may state the

As online reviews become more popular, there is no way for law firms to opt out. Clients are already posting reviews of attorneys on a number of different websites.

firm's practices and policies with regard to the issue raised, and, if appropriate, encourage the dissatisfied client to contact the firm directly to resolve the issue. This type of response shows that the firm respects confidentiality and takes client satisfaction seriously, while providing a professional statement on the issue raised.

Asking for positive reviews

The best thing a law firm can do about negative reviews online is make sure they constitute a small percentage of the total. The attitudes of consumers toward reviews are no different for legal services than for other goods and services. If a large percentage of the reviews are negative, or the overall "star" rating is low, this gives the consumer pause. However, when reviews are overwhelmingly positive, then one or two negative reviews will be ignored. To generate that abundance of acclaim, attorneys must overcome the tendency of the satisfied consumer to stay quiet.

People turn to the Internet to complain far more often than to praise. To be satisfied is to have one's expectations fulfilled, and have no further need. Satisfaction is the desired state, and it does not spur action. However, it does not take much to get a satisfied client to express themselves in an online review. All you have to do is ask.

Of course, attorneys must follow their state bar rules regarding ethics and attorney advertising. The bar rules for different states may prohibit giving anything of value in exchange for a review, and some may ban solicitation of reviews entirely. In addition, law firms should follow the rules of any third party websites for which they are soliciting reviews. Some websites, notably Yelp, state that businesses should not ask people to post reviews. The algorithms employed to detect improper or fake reviews are becoming

RESPONDING TO NEGATIVE REVIEWS PROPERLY IS IMPORTANT, BUT IT CANNOT BE REACTIVE. LAW FIRMS SHOULD ALSO HAVE A STRATEGY FOR GENERATING POSITIVE REVIEWS FROM CLIENTS.
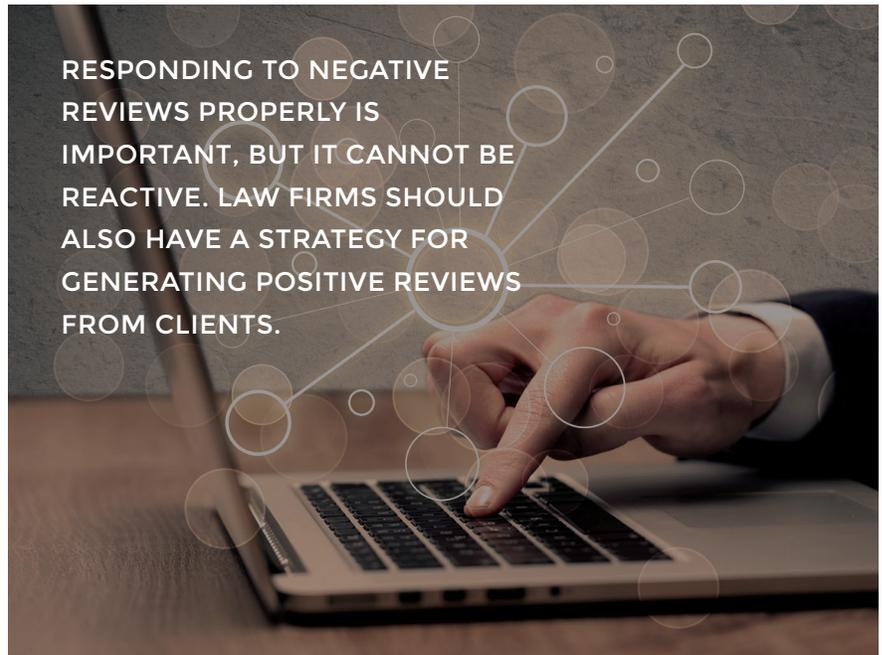
more sophisticated, which rewards businesses that follow the rules.

Assuming that all applicable rules are being followed, just how does a law firm go about asking a client to say something nice about them? The first consideration should be obvious: Only ask happy clients for reviews, and ask them when they are happiest. Many clients, upon receiving a large settlement check, tend to start thinking their lawyer is pretty great, and that is the perfect time to ask. Of course, not every field of law lends itself to such happy moments, but firms can solicit reviews from their most satisfied clients at a time when they are feeling the most positive.

Not every client will agree to post a review (and not all those who agree will follow through), so it is important to make the request part of the firm's normal procedure in successful cases. Asking in person may be effective sometimes, but it also makes sense to solicit an online review as part of a final letter or email to the client. This provides a reminder for those clients who may actually follow through, and it allows

clients who do not wish to review the firm to ignore the request without feeling pressured. Asking for a review may not seem like the most important task on an attorney's agenda, so asking in writing as part of the firm's standard procedure also ensures that requests are made.

The final essential element in getting happy clients to leave positive reviews is to make it easy. Do not overwhelm them with options. Instead, present the client with an easy link, directly to the place where you are asking them to write the review. Your firm may wish to create a webpage with a URL that is easy to remember, like yourfirm.com/review. That page should have one or more big buttons that connect the client directly with the review form for your firm on Google, Avvo, Facebook, or another review site. The firm's own data will help determine which of these review sites to focus on, but at present Google reviews are of dominant importance.

A law firm's online reputation is vital to success. Make sure your firm has a five-star strategy for online reviews.

- Brendan Conley

Mobile Security
Don't let your firm be hacked with an SMS

With offices moving to the cloud, more lawyers are using their own hardware to stay productive while away from the office. Merging personal and professional data on the same device opens both sides to cyber attacks.

Most workplaces are fully online: Printers and landlines are networked, paper files are being digitized and indexed for searching, and business services are accessible from a wide range of browsers and dedicated apps.

A recent model iPhone or Galaxy S phone has roughly the same computing power as a desktop computer did 5-10 years ago. Many modern phones are able to run the same apps, receive email and access company resources with only a few minutes of setup. The traditional office, which does not rely on intense local computations, can fluidly work between desktops and phones without skipping a beat.

Almost half of all U.S. jobs can at least partly be performed remotely, and 80 to 90 percent of the working population has some desire to do their jobs remotely. Of 200 U.S.-based workers surveyed by TheEMPLOYEEapp's second annual study, 40 percent

of the respondents work in a non-traditional setting and 55 percent indicated they travel. To remain connected, 49 percent use smartphones and 28 percent use tablets in their work.

Additionally, 70 percent of those surveyed are using their own personal devices. The survey revealed many did so without their employer instigating a proper mobile policy. It is the working population that is using the device they purchased for personal use and are plugging it into their company's cloud and intranet.

This is a nightmare scenario for information security. Without a proper device policy, which includes technical oversight as well as security training, your phone is exponentially more dangerous to both the office and home. Moreover, the sensitive and protected nature of the data contained in a law firm can fetch a large bounty for would-be hackers.

Something as simple as viewing a webpage on your phone requires hardware and software from dozens of technology vendors. With so many moving parts and varying levels of security, hackers have their pick of where they want to start. They can target you, your workplace or even the routers that move every 1 and 0 across the internet. Here are a few ways prying eyes find what is not meant to be found.

PINs and passwords

Passwords are both the greatest deterrent against intruders and also the reason many hackers are successful. An IT analyst collected troves of publicly available leaked passwords, sampled the data and extrapolated 10,000 most commonly used passwords. The takeaway from the results is that people are terrible at coming up with passwords. The most effective solution to the password problem is to increase the entropy (or measurable strength) of a password so that it is no longer cost effective to try to guess.

It is no help that many sites will enforce seemingly arbitrary rules which result in complex or instantly forgotten passwords, which are then changed to weak ones. PIN codes are being treated in the same way with a significant portion of the population using straight lines or even just repeating the same four numbers.

Password cracking is more effective than ever. With each leak, patterns are fed back into the software to improve its effectiveness. One specialized cracking cluster was able to generate 350 billion guess per second, and this was back in 2012. More people are using passwords that are easier for machines to guess but harder for humans to remember.

Another possible weak point for passwords is sharing them by sending them over email, or even writing them down. It is a dangerous way to approach security: A login with more than one co-worker will often have an easy to remember but very insecure password.

Several password managers like LastPass and 1Password will do the work of creating, storing and changing your passwords to ones that are mathematically challenging. They are built for office environments with strict policies over who can use what password but remain flexible enough to fit most situations. You are still responsible for securing the master password but that could prove easier than trying to manage every site from memory (or worse, pen and paper).

Software or hardware vulnerabilities

Another angle of attack is to go after vulnerabilities in your handset or the software you use. Closed source software and open source software are both targets of such exploits. Adobe's Flash platform is notorious for being targeted and exploited on a regular basis. It has gained such a bad reputation that Adobe has changed the name of their publishing software to Animate, which can still be used to render animation to safer formats such as MP4 or HTML5. Flash should be disabled from running or uninstalled completely from your system as exploits have been known to circulate for days before Adobe is made aware of the issue and can attempt to push a fix.

Even with companies investing more than ever into IT infrastructure, bringing your own device usually means bringing your own security policy. Not everyone wants to update their software the moment they receive that update notification, and many do not.

Outdated software is probably the most dangerous and easiest thing to infiltrate, because its weaknesses are known. If an update for a WordPress plugin promises to fix an exploit in a certain part of the code, then sure enough, armies of bots will crawl the web looking for older versions and attempting to use published vulnerabilities.

Before these vulnerabilities are patched, or even known to the vendor, they are called "zero day" exploits. Zero days have great appeal and value to hackers since they allow hackers to infiltrate and cause devastation without being detected for some time. Criminals are not the only ones accessing systems and hardware without detection; as recent leaks have shown, government intelligence agencies have employed the same methods for years.

Earlier this year, Apple made headlines by rejecting a court order compelling it to assist the FBI in decrypting the phone of a deceased terrorist. The refusal from Apple was not a knee jerk reaction, but a stern warning that any backdoors in encryption would ultimately end up in the wrong hands, nullifying everyone else's protections.

Surely enough, these fears were confirmed when a huge cache of spying and hacking tools were leaked

online and ultimately confirmed to belong to the NSA. Instead of attempting to snoop on individual machines, programs with names like BANANAGLEE and SECONDDATE targeted various weaknesses in industry standard routers, allowing them access to intercept traffic to their own servers.

Support exploitation and human manipulation
Even though your firm may not be the target of government sponsored spying or a large scale botnet attack, there is always a chance that a curious individual just wants to see how far he or she can go. Rather than trying to break your digital or physical security head on, they would look for someone on the inside who could let them right in.

One of the most notable cases of identity theft happened to Mat Honan, a technology writer for Wired. It occurred almost entirely over the phone, with the culprit calling Apple claiming to have trouble logging in and then being provided a temporary password. This happened in 2014, but it has not prevented similar incidents occurring with banks, cloud providers and cell phone companies.

One popular Youtuber Ethan Klein nearly had his channel of 2 million subscribers deleted, when someone posed as a T-Mobile employee helping Ethan get a new SIM card. They were successful and gained access to his entire contacts list. More valuable was their primary goal of being able to intercept his two-factor authentication texts. Ethan was familiar with this type of attack and quickly acted, when his phone lost all service, recovering his SIM before further damage could happen.

These social engineers have familiarized themselves with corporate structures and policies and know exactly how to extract

the information they need. It all starts with a simple email, carefully researched and formatted to look like someone in your contacts. In the case of Snapchat, an email was spoofed from CEO Evan Spiegel requesting payroll information for existing and ex-employees.

Safer Handling of Handhelds
Any devices integrated to the office intranet should be updated to the latest versions. Both Android and iOS have suffered from SMS exploits which give complete control over the device. The latest versions address this bug, and many more, yet Android's inability to update on older devices still makes it a prime target.

Biggerlawfirm.com received almost 10,000 login attempts in the month of July alone. Having strong passwords, or a password manager that handles this, is the way to make sure password guessing bots never get it right. Your phone's unlock PIN should never be a recognizable pattern such as a line, four corners or repeating numbers. Enabling the destruction of your data with too many wrong guesses should be mandatory.

Perhaps the best mobile policy is having an office culture that embraces security. We all know not to give out personal information to telemarketers whom we know nothing about, but how suspicious would you be if the partner attorney asks for information they would not normally ask for?

There will never be such a thing as perfect security. Even after establishing a personal device policy, make sure it is easily accessed and understood by all employees, and constantly put it under review. A policy that fits your firm best and changes with your history and future needs ensures your reliance on technology is a healthy one.

- Justin Torres

ANTICIPATE THREATS TO YOUR FIRM'S SECURITY

PINS AND PASSWORDS
Password cracking is more effective than ever. With each leak, patterns are fed back into the software to improve its effectiveness. Arbitrary password rules on some websites force users to pick passwords that are harder to remember but easier for machines to guess.

SOFTWARE AND HARDWARE
Outdated software is probably the most dangerous and easiest thing to infiltrate, because its weaknesses are known. Closed source software and open source software are both targets of such exploits.

SUPPORT EXPLOITATION
Hackers have familiarized themselves with corporate structures and policies and know exactly how to extract the information they need. It all starts with a simple email, carefully researched and formatted to look like it came from one of your contacts.

UNWITTING USERS
Even with top of the line hardware and software defenses, users of technology can unknowingly be the weak security link. Introducing personal devices into the workplace can be a boon for employee productivity and job satisfaction, if done with a proper mobile security strategy in place.

Marketing helps keep a law firm alive, thriving and viable.

Digital Asset Management
Are you keeping track of your firm's brand?

In a highly competitive marketplace, your firm needs to regularly produce interesting and focused legal content. That legal content – videos, papers, ebooks, brochures – should be high-quality and consistent.

Legal marketing is an ongoing task that requires ready access to a variety of digital assets. Most law firms have a collection of items that are used for various marketing purposes, ranging from logo files to candid photos of charity and speaking engagements. Some of these assets will be needed for brochures, business cards and others for press releases, videos and online marketing. All of these assets should be easily accessible, well-documented and ready for use, either internally or by a contracted marketing company.

Digital asset management is an important and often underappreciated issue facing law firms. Managing marketing content materials is not the same as managing client resources. Over years of operation your firm will likely have compiled more resources than you know, and when it comes to finding a specific asset, like an original logo file, things can get complicated.

If not the filing cabinet approach, what about software to solve the problem?

Managing brand assets is a big task. Assets include any items that are used to identify a firm, like fonts, colors, podcast sound tracks, logos, photos, videos, music and document templates. Anyone using these resources must know the standards of their

use. What fonts are acceptable for use in presentation slides, and in what combinations? What colors can be paired on a web page? What is the difference between a web and a print file? What types of stock photography can be used in a brochure? These are all questions that brand management — and digital asset management solutions — can answer.

Keeping track of all marketing material helps maintain a firm's brand consistency. Due to the large quantity of digital content, however, firms cannot store, recall and work efficiently with contractors. A lack of efficiency can result in errors of recreation done by a marketing company or website designer. Ultimately, this results in noticeable inconsistencies and poor branding. Any company a law firm is working with to produce marketing content needs to be on the same page — and have access to the same files. Therefore, digital assets need to be safely stored and easy to find by anyone in the office.

DAM – brand management system that works

DAM stands for digital asset management, a hot trend for 2016 and a good idea for law firms. It is software that manages branded content assets from start to finish. DAM software goes beyond the standard filing system that you

use when storing documents on your office computer or in the cloud. It is an interactive, dynamic delivery and storage system that allows anyone at the firm to categorize, store and locate digital assets in a few mouse clicks. It is a system worthy of the challenges faced by law firms looking to grow, increase their efficiency and effectiveness when it comes to brand management and consistency.

With DAM software, a firm can tag content in any way members find convenient, such as by event, year, topic or type of content. These tags are then used to search for and locate files for future use. User permissions can be assigned at a management level, so everyone in the office has access only to the resources they will need to use.

Additionally, users can archive outdated content to make certain it is not used for a new project, but is stored for use if needed again. DAM can aggregate data from several points within the system to pinpoint patterns for all content types. Knowing what material is used frequently and what needs refreshing is helpful when keeping track of digital assets.

A downside of moving to an asset management technology is the organization and set-up time. These solutions are not plug and play. To effectively use the system, your firm will need to collect, tag and describe all of its content. You will need to develop a naming system that can easily be shared with new staff and associates. And, most importantly, you will need to create a set of brand standards and guidelines, so that those who have access to the files know how they should be used.

Do we really need all this?
Before you consider investing in digital asset management, you need to examine not only who is going to use it but also who is going to manage it and keep the firm on track in developing new marketing materials. Someone, with

marketing technology experience, must be responsible for advocating and moving the system and process forward. DAM is just one part of the big picture in keeping law firm marketing on track.

What about just using cloud storage?
Cloud storage systems like Dropbox allow for the secure storage, sharing and organization of digital assets. But digital brand management software contains features that go farther. Digital asset management is not just storage, it is a brand guidelines system. It is a resource that allows you to define and organize your brand and any assets associated with it. It allows you

> Keeping track of all marketing material helps maintain a firm's brand consistency. Instead of labelling files arbitrarily and hoping to recall the name of the file at a later date, use a digital asset management tool, which makes finding any file as easy as a few clicks.

to store things like colors and color palettes that simple cloud solutions are not built to handle and to group them visually with logo files and images for use in projects. Some of the additional features DAM solutions offer include:

- The ability to create collections, so all elements needed for a specific type of presentation are in one place

- Online simple file editing, like cropping, rotating, and flipping

- File expiration dates, for assets that should only be used for a specific amount of time

- Enhanced administration functions, like user-level role management and the ability to create file discussions

- Online brand guideline hubs

Is DAM right for your firm?
Digital asset management software is a time and cost investment. Software options vary in price and pricing structure, and many are targeted at enterprise-level organizations. Solutions built for large firms, which offer access from 15 to 50 to unlimited users, range from around $400 to over $1000 a month. Some, like AssetBank offer a permanent license, but the lowest price for such a license is $7000 (for up to 50 users).

Other companies target firms with fewer employees. For example, Intelligencebank, which charges from $9 to $19 per user per month. For a firm that has only a handful of people managing marketing resources, a system like this could be manageable.

Your law firm can likely find alternatives to DAM software. If you decide that the investment is not right for your firm, you should still create and maintain a system for managing brand assets. Everyone at your firm, and any agencies that work with your firm, should understand the basics of your brand and marketing strategies. Additionally, everyone who is involved in producing marketing materials should have easy access to high-quality files, fonts, print and web color palettes so that your firm will portray a consistent, professional image across all platforms.

Finding items for projects without some form of a management system can be a major setback to getting a project done well. Triggers such as a merger or acquisition, rebranding, a change of managing partner(s), a change of location, a change in practice areas or new attorneys often bring to light old digital assets that need to be updated and organized. It is best not to wait for a shake-up to force your hand.

- Kerrie Spencer

Are you competing against your marketing company?

BRISKMAN BRISKMAN & GREENBERG ISN'T

CUSTOM
LEGAL MARKETING

If your marketing company isn't exclusively working for you, they're helping your competitors. That's why Briskman Briskman & Greenberg trusts Custom Legal Marketing. They know Custom Legal Marketing won't work with any competing firms in their No Competition™ Zone.

Secure your law firm's No Competition™ Zone at customlegalmarketing.com/exclusive

No Competition™