How Cyber Threats Affect Law Firm Marketers

Stories of cyber hackers penetrating credit bureaus, government resources, corporations, social media sites and even law firms continue to highlight the ever-growing threat to organizations that operate in a digital environment. For years, law firm technology has lagged behind the majority of corporate America. Some firms have been slow to secure their IT environments, leading to data breaches that wreak havoc on a firmâ€™s public reputation, increase liability and expose the firm to potential data privacy lawsuits from clients whose information was not protected properly.

In January of 2017, news of the first public data security class action complaint against a U.S. law firm was made public. This may be the first of many future actions against law firms that fail to properly secure sensitive client data.

Melanie Trudeau
Vice President
Digital Marketing
970.376.7746
mtrudeau@jaffepr.com

Understanding the Severity of Cybersecurity Threats to Law Firms

Even though law firms generally manage retail-type websites (in other words, law firm sites are not usually e-commerce sites), they are far from immune to cyber threats. In fact, firms are prime targets for cyber criminals. Attorneys store sensitive information such as trade secrets and other intellectual property, market-moving deal news, employee information, and internal financials that can be highly valuable to cyber hackers. From insider-trading opportunities to abuse of proprietary IP information and confidential client communications, data breaches can result in a vast swath of criminal activity.

Not only can a cyber attack on a law firm lead to security risks for clients, but it can also create reputational damage to both clients and their lawyers. In an industry where confidentiality is at the core of client service, any whisper of cyber vulnerabilities will inevitably create grave concerns among clients and potential clients.

How Do Cybersecurity Risks Affect Legal Marketing?

Maintaining rigid cybersecurity best practices generally falls on a firmâ€™s IT department or outside vendor; however, law firm marketers still need to consider the following aspects of data protection and cybersecurity risks.

Consumer Confidence

Consumer perception of weak security practices influences consumer confidence. Simply put, if potential clients think their sensitive information is at risk, they will go elsewhere for legal services. Gemaltoâ€™s 2017 Data Breaches and Consumer Loyalty report reveals

that 66 percent of consumers would be unlikely to do business with organizations responsible for exposing financial and sensitive information.

Bolstering consumer confidence starts with a professional, up-to-date website. As the virtual â□□front doorâ□□ (and ideally not the â□□back doorâ□□) to your law firm, your website cannot appear to be built by your IT managerâ□□s 12-year-old child.

Law firm marketers must work with their IT departments/vendors and web developers to ensure their firmsâ□□ websites follow best practices for data security. This may include purchasing an SSL certificate, avoiding outdated coding, running regular CMS security updates and avoiding any weaknesses where hackers could penetrate your site. In addition, your hosting company or internal servers have to be secure. Persistent downtime and crashes are indicators to web visitors that something on your website might not be safe. Even an outdated website design or lack of a mobile version can send up red flags to consumers worried about cybersecurity.

Ongoing cybersecurity measures may require monitoring services to help with intrusion detection, data leakage, email filtering and virus protection. These extra layers of protection will help uphold consumer confidence in your firmâ□□s cybersecurity capabilities.

Cybersecurity Communications to Clients

With the increased media attention around cyber attacks comes an increase in demand for information about a firmâ□□s data security policies and procedures. Seeking assurances that their confidential information is safe with their attorneys, clients are requesting audits and guarantees that a firm follows stringent standards for cybersecurity.

The marketing department is often tasked with communicating the firmâ□□s cybersecurity policies and procedures to clients and prospects. Firms with robust cybersecurity measures in place should be leveraging their data protection capabilities to establish a differentiator among competitors. Determining how, when and where this message is conveyed falls on the firmâ□□s marketing department. Keep in mind that the average person does not understand the language of IT experts. The firmâ□□s cybersecurity measures have to be clearly explained and delivered so clients and prospects donâ□□t feel like they are being misdirected by complicated, technical language.

Crisis Communications Plan

As with any issue of potential risk, a law firm must have a solid crisis communications plan that outlines the firmâ□□s internal and external response to a cyber breach. Some say a cyber attack is no longer a question of â□□if it will happenâ□□ but of â□□when it will happen.â□□ Outlining a communications plan before an attack happens, and keeping it up to date as the digital landscape changes, requires input from various firm resources.

Work with your IT department to make sure your marketing committee or department understands the full implications of a cyber breach and the steps required to restore protections. Be aware of the potential consequences of client data landing in the hands of cyber criminals. Often, the full implications of a data breach are not realized until well

after the breach happens. Preparing a crisis communication plan will at least empower your firm to stay on top of a crisis.

Cybersecurity Resources for Law Firms

Resources are available to help your firm keep its cybersecurity efforts current.

The ABA has created a cybersecurity legal task force that provides cyber alerts, legislative updates and recent cyber news to help law firms navigate the ever-present threat of cyber attacks.

The Global Resilience Federation formed a Legal Services Information Sharing & Analysis Organization where â members are â trust-sourcingâ threat indicators for analysts to research, scrub and anonymize, yielding actionable intelligence for dissemination in real-time.â More than 100 law firms have joined the organization to share information and flag potential threats and system weaknesses.

This article originally appeared in the ALM publication Marketing the Law Firm *in the June 2018 issue.*