In the crosshairs:
Cybersecurity for law firms

Time to invest?
Making the most of a budget surplus

How to uncover and end
billing fraud at your firm

Be sure your website
is pulling its weight

LAW FIRM MANAGEMENT

FALL 2018

990 Stewart Avenue
Garden City, New York 11530

t: 516.288.7400
f: 516.288.7410
e: info@garibaldicpas.com

GARIBALDI GROUP
Certified Public Accountants
Financial and Management Consultants

www.**garibaldicpas**.com

In the crosshairs: Cybersecurity for law firms

The leak of the so-called Panama Papers, 11.5 million documents with financial and legal information stolen from an international law firm, made headlines around the globe in 2016. While the well-known names included in the papers were the focus of many news stories, the hacking incident also highlighted the cyber risks confronting law firms of all sizes. Yet many firms continue to lag behind other businesses when it comes to taking the measures necessary to prevent and mitigate attacks.

THE CURRENT LANDSCAPE

One reason many firms are behind the curve on their cybersecurity: the cost. The minimum defense — security-focused software — can be expensive. But cost justifications fall in the face of the risks.

As the American Bar Association (ABA) has pointed out, law firms are cybercriminal targets for two reasons:

1. They gather, store and use highly sensitive client information while at times using safeguards inferior to those of their clients.
2. This information is more likely to be of interest to a hacker and likely represents a smaller amount of information than the client has.

The ABA categorizes hacking and data loss in terms of "when," not "if." Clients seem to be coming to the same conclusion. They've begun to demand certain levels of data security and include such specifications in their retainer agreements (sometimes unbeknownst to their law firms until too late).

THE ETHICS ELEMENT

Effective cybersecurity is more than just a smart business practice — it's also a matter of ethics. Bar associations have recognized the cyber risks attorneys bear and increasingly are moving to address the issue with rules and opinions.

For example, the New York County Lawyers Association issued an ethics opinion in 2017 that says the New York Rules of Professional Conduct require lawyers to stay current with technological developments. Moreover, the opinion states that a lawyer's "duty of technological competence may include having the requisite technological knowledge to reduce the risk of disclosure of client information through hacking or errors in technology. …"

The American Bar Association also tackled cybersecurity in 2017, in its Standing Committee on Ethics and Professional Responsibility Formal Opinion 477, *Securing Communication of Protected Client Information*. It adopts a "fact-specific approach to business security obligations that requires a 'process' to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments."

Others are taking more drastic steps to protect themselves. In 2016, for example, a class action lawsuit was filed against a Chicago firm based on its "practice of systematically exposing confidential client information and storing client data without adequate security." Notably, the firm hadn't actually been hacked and had suffered no known data breaches.

Firms that have been attacked have incurred a range of damage. In addition to the loss of confidential files and information, cyberattacks can lead to downtime and loss of billable hours, costly mitigation and recovery efforts, higher insurance rates and long-lasting reputational injury.

Despite these risks, a 2017 ABA survey found that only 26% of respondent law firms had a data breach incident response plan in place. Of firms with two to nine attorneys, 14% had the plans, and only 10% of solo practitioners had them.

PROTECT YOURSELF AND YOUR CLIENTS

At a minimum, law firms should incorporate the following security measures into their way of doing business:

Training. The Ponemon Institute, an independent researcher on privacy, data protection and information security policy, has found that negligent insiders are the root cause of most data breaches. One unthinking click on a link in a phishing email, for example, could unleash malware that paralyzes the entire firm. And the risks are exponentially higher when employees work remotely via multiple, easily misplaced or stolen devices, often over vulnerable public Wi-Fi networks. Employees must receive regular training on the risks and how they should handle them.

Encryption. Encryption is nothing new, but many law firms haven't adopted it on the widespread basis that they should. Perhaps the lapse is due to the time and expense previously involved in establishing encryption, but the process is quite simple and cost-efficient these days. Firms should require whole-disk encryption of every desktop or laptop computer, mobile device, USB flash drive and hard drive used to store data.

Patches/updates. Yes, it can be a pain to keep up on updates to the operating system or software. But it's important to remember that such updates and patches usually are released in response to the discovery of security vulnerabilities.

Incident response plans. The 2017 ABA survey showed an improvement in the number of firms with plans, but many remain without a roadmap for how to respond to an attack. Your plan should clearly describe the individual roles (and name the respective attorneys and other employees) and the processes and procedures to be implemented. It should be concise and immediately actionable when needed.

THE TIME IS NOW

Law firms that relegate cybersecurity to the IT department or think of it as a one-time project make a serious mistake. The risk — and the steps to mitigate that risk and recover when disaster strikes — call for an ongoing, firmwide effort. •

Time to invest?

MAKING THE MOST OF A BUDGET SURPLUS

With the economy thriving, many law firms find themselves with a budget surplus for the first time in several years — possibly the first time this decade. If you're one of these firms, consider investing some of those funds in achieving long-term growth.

INVESTING VS. BORROWING

Borrowing can seem like the preferable option, but borrowing comes with costs. And even in a time of relaxed regulation, many banks have strict lending and underwriting policies. Some partners may want to go the financing route to avoid cutting into their profits, but lenders can have surprisingly tough expectations regarding partner-invested capital.

In addition, lawyers are often private people. Financing means opening up the firm to oversight by and reporting to the lenders. Lenders also might require personal guarantees from the partners.

TALENT ACQUISITION

So what should your firm invest in? This is a great time to build up your bench of talent, whether by adding experienced lateral hires, bringing on attorneys fresh out of law school, or adopting some combination. The former requires upfront investment in recruiter fees. New attorneys require an investment in training.

New lawyers and laterals can help a firm fill holes in lucrative practice areas, line up successors to Baby Boomers eyeing retirement and build new practices in emerging areas. It all comes at a cost, but it's essential to maintain or increase revenues.

OPERATIONAL IMPROVEMENTS

Law firms have long sought to plant offices in new markets and expand facilities in existing markets. Office-related costs — whether buying, leasing or establishing virtual offices — remain significant and are better taken on when a firm is in the black.

Technology costs continue to rise, too. But few firms can afford to fall behind in today's tech-driven business and legal environment. Firms sitting on a surplus should re-evaluate (or develop) their technology plan to stay current with recent advances and client requirements.

Technology investments can, of course, rapidly become obsolete. Realistically assess your current and medium-term needs and conduct extensive

research before sinking money into new tools. With informed investments, though, a firm can likely improve both its delivery of services to clients and its back-office work (for example, billing, invoicing and document drafting).

BUSINESS DEVELOPMENT

It's been said that you must spend money to make money, and that is certainly true for business development efforts. Gone are the days when informal networking at the club or on the golf course was enough to generate sufficient new business.

Savvy firms now invest heavily in business development. This includes purchasing proven customer relationship management technology, hiring marketing professionals, and advertising where appropriate.

PLAY THE LONG GAME

Attorneys often fixate on annual profits, viewing vital investments that promise long-term returns as short-term expenses that cut into their immediate bottom line. For your firm to remain competitive and sustainable, though, some strategic investment is essential. •

How to uncover and end billing fraud at your firm

Most attorneys would be adamant that their firm bills clients appropriately — no padding time records, exaggerating expenses or performing unnecessary work to bill a client more. Yet, it occurs over and over, maybe while partners look the other way at questionable billing habits from either a lone attorney or a larger subgroup at the firm.

This will open the doors to disciplinary action and litigation, not to mention public injury to a firm's reputation. So it's critical to uncover and end any billing fraud that might be occurring in your firm.

WHO'S RESPONSIBLE?

While anyone at your firm, including partners, associates and paralegals, can falsify timesheets, your billing partners and administrators ultimately are responsible for ensuring that bills are accurate and fair. If your billing partner regularly "rubber stamps" time records, you need to change that.

Create — or update — a bill preparation checklist and require everyone responsible for billing clients to follow it. While your firm's practice type and fee methodology will determine specific areas of vulnerability to billing fraud, billing partners and administrators should be on the lookout for the following:

Incomplete descriptions. Cryptic or incomplete summaries of services aren't unethical, but they may be suspicious. If an attorney billing big hours appears to cut and paste a handful of nonspecific descriptions such as "E-mail client," or "Phone conference with associate," ask him or her to provide more explicit summaries that can be verified as actual client work.

Math mistakes and rounding errors. Everyone makes an occasional math mistake. Review bills from lawyers who regularly submit bills with hourly totals unsupported by line items. Also flag attorneys who bill only full or half hours (as opposed to quarterly or 10-minute increments) or who bill close to the same number of hours every day.

Extra hours. It's not unusual for lawyers to put in extra hours as a case nears trial or a deal approaches closing. But if an attorney routinely bills 12 to 15 hours a day, something may be amiss, particularly if other lawyers are leaving at 6:00 p.m. every night.

Expense padding. One of the most common ways lawyers bilk clients is by padding their expenses. Train your accounting staff and billing partners to spot inflated amounts, falsified receipts and personal charges marked as client-related expenses.

Train your accounting staff and billing partners to spot inflated amounts, falsified receipts and personal charges marked as client-related expenses.

WHAT ABOUT FIRM CULTURE?

Scrutinizing time and expense reports for inaccuracies is only one element of preventing billing fraud. Falsified bills may arise from deeper cultural problems, including unrealistic performance expectations and tolerance for unethical behavior.

How many hours do you require of associates? Setting the bar too high may induce an attorney to falsify billing records to meet the target hours. Some critics assert that the billable hour (and compensation models that reward top billers) encourages cheating. Others claim that some lawyers will cheat regardless of billing methodology, particularly in times of economic insecurity or when under personal financial pressure.

WHAT CAN YOU DO?

The most important step a firm can take is to set the proper tone. Firm leaders need to foster an ethical environment. To start, provide and require ethics training for new employees. Then set reasonable expectations for both workloads and performance. Be sure to compensate partners and employees for ***quality*** as well as quantity.

Importantly, encourage both employees and clients to report potential billing fraud, and protect whistleblowers from reprisal. Finally, managing partners and other leaders need to ensure that their own words and conduct — whether with clients, colleagues or employees — are above reproach.

WHAT YOU CAN DO NEXT

While some bill padding incidents are open-and-shut cases of fraud and need to be handled as such, other incidents are murkier. So don't automatically assume fraud is occurring. For example, sometimes legitimate services may be billed for more hours than is customary. The issue might not be fraud but time management. In that case, the solution could be providing the attorney with time management training. •

Be sure your website is pulling its weight

Law firm websites have been considered a must-have for years now, but it's one thing to have a site and another to have a site that's benefiting the firm. Which kind of site are you operating?

METRICS THAT MATTER

Several metrics can help you assess whether your firm is getting its money's worth from a website.

Visitors. The most obvious measure for evaluating a website is the number of visitors it draws. But don't stop there. How many total visitors did the site get for a specified period? Is the number moving upward or at least holding steady?

Consider the number of first-time visitors. Comparing new visitors with total visitors indicates how many people return to the site. A slew of new visitors may suggest a recent social media or other marketing campaign is working. A high number of returning visitors might show the site's content is strong and generating leads.

Track the sources of site visitors. Direct visitors enter the URL in their browsers, while organic search visitors arrive through a search engine's list of results. Referrals click a link to the site from another website. And social visitors come via links on social media platforms.

Time on site. Generally, the longer the duration of a visit, the better. But lengthy visits could also mean the site isn't user-friendly, and visitors have a hard time finding information. In such cases, visitors are generally more likely to leave a site in frustration than continue to search.

Pages per visit. How many pages on the website does the average visitor view on a visit? Compute this figure by dividing the total page views by the number of visitors. A high pages-per-visit number usually signals strong content.

Bounce rate. Equally important is the number of visitors who leave the website after checking out only one page. Firms might reduce this bounce rate by improving navigation and internal linking. Along with time on site and pages per visit, bounce rate reflects the extent to which visitors are engaging with the site, instead of dropping in and quickly exiting.

Conversions. This refers to visitors taking action on a website. They may download a white paper, sign up for an email newsletter, request more information or schedule an appointment.

DO THE MATH

Done right, a law firm website can pay off. But a neglected site quickly becomes a sunk cost. It's up to you to do it right. •

GARIBALDI
GROUP
Certified Public Accountants
Financial and Management Consultants

990 Stewart Avenue | Garden City, New York 11530

PRSRT STD
U.S. POSTAGE
PAID
CHICAGO, IL
PERMIT NO. 4269