LEGAL MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

LI Feature

LEGAL INDUSTRY/BUSINESS MANAGEMENT

Cyber Breach: The Risk Is Now Reality

The legal industry has been cited as a target for hackers. How ready is your firm?

Risk management for a law firm today involves much, much more than the risk of malpractice lawsuits, conflicts of interest and the usual risks covered by insurance (property and casualty, general liability, business continuity, etc.).

JACK M. VAUGHAN & EBEN KAPLAN

Vaughan *(left)*
Risk Management Consultant

Kaplan *(right)*
Senior Consultant
Control Risks

Today, a law firm faces the very real, pervasive and potentially catastrophic risk of a cyber breach — an intentional invasion of its treasure trove of highly confidential, sensitive, proprietary and often *privileged* client and employee information.

An excellent article on this subject appeared about a year ago in this ***publication***. But guess what? The problem (and the risk) has gotten worse, much worse, in only 12 months!

Cyberattacks against law firms are nothing new. The Federal Bureau of Investigation (FBI) began warning firms that they specifically were being targeted by organized cybercriminals as early as 2009. In 2011, they invited 200 of the largest law firms to discuss the rise in sophisticated cyberattacks targeted at law firms. Part of the reason is that law firms often present an easier target than some of their clients; if a hacker wants to steal sensitive information from a company, he or she may have better luck going after that company's outside counsel.

QUICK HIT 1

This is the first year that the legal sector appeared on Cisco's annual ranking of industries targeted by hackers, debuting at **No. 6**.

This is the first year that the legal sector appeared on Cisco's annual ranking of industries targeted by hackers, debuting at No. 6. And law firms' clients are taking notice. Many financial institutions now require law firms to complete checklists and subject themselves to audits of their information security apparatus.

Most decline to speak publicly on the issue, worrying that it puts them out there and might "paint a bull's-eye on [their] back."

One representative from an AmLaw 100 firm, who prefers to stay anonymous, says as far as cyber breaches are concerned, all firms are at risk.

"We as organizations have to accept that basic fact, and prepare accordingly. No firm can assume they aren't a target and approach security in a casual manner. It just doesn't work, given client's expectations in this area today and what is truly at risk. Just look at the outside counsel guidelines firms receive and what clients are focused on. And while I think all firms would say they understand that fact and are dealing with the issue, my belief is they aren't always doing all they can."

QUICK HIT 2

For most firms, dealing with a cyber breach is not a question of "if," it's a question of "when." Firms that prepare themselves for this eventuality can greatly limit the impact when a breach does occur.

CYBERATTACK: NOT IF, BUT WHEN

Law firms have an ethical and professional duty to make all reasonable efforts to protect the information they hold. Remaining the weakest link protecting their clients' data is an unsustainable proposition. Not only does it expose firms to considerable liability, but it also threatens their ability to retain their clients.

In this context, cybersecurity ceases to be an issue just for the IT department and becomes an issue requiring attention from the highest levels of leadership. If your firm's managers are not focused on cybersecurity, they need to be.

For most firms, dealing with a cyber breach is not a question of "if," it's a question of "when." Firms that prepare themselves for this eventuality can greatly limit the impact when a breach does occur. In fact, one source notes that his firm focuses significantly more attention and resources on early detection and response.

The starting point for a comprehensive information security plan is a **risk assessment**. That sounds basic, but too many firms essentially skip over that fundamental step and start implementing security safeguards and tools without first stopping to consider what it is that they are protecting and from whom they are protecting it. Not all information requires the same treatment, and only after a firm has identified which types of information are the most sensitive can it begin to make decisions about safeguards. Likewise, knowing who might be after your information can greatly inform your defense — targeted attacks can be met with targeted defenses.

QUICK HIT 3

The starting point for a comprehensive information security plan is a risk assessment. That sounds basic, but too many firms essentially skip over that fundamental step and start implementing security safeguards and tools without first stopping to consider what it is that they are protecting and from whom they are protecting it.

This is not to suggest that firms should ignore basic prevention measures — firewalls, password management, email safeguards, end user training and awareness — that are essential to harden a network's perimeter defenses. But these should be complemented with inward-facing measures that concentrate on detecting a breach before the intruders can do any damage. In addition, firms should **limit user access to highly sensitive matters**, such as merger or acquisition matters and high profile litigation disputes. Only the attorneys working on these matters should be given access to the documents and data.

According to one AM100 Law Firm Chief Operating Officer, who preferred to stay anonymous, "a multi-tiered approach is key in identifying suspicious activity. Also important is establishing appropriate alert thresholds and reacting immediately to those alerts. Ideally, if you are using multiple systems, it is best to feed them in to a single correlation engine, which improves the value of the alerts as well as provides a single view into events," he says.

"User education is also critical, since most of today's breaches occur as a result of something a user did or did not do."

NOT JUST A MATTER OF PREVENTION

It is no longer sufficient to have an information security posture built solely around prevention. Spear phishing attacks have gotten so sophisticated that even the most alert and paranoid users have little chance today. Hackers go to incredible lengths to make their come-ons look legitimate in the eyes of a target — they'll do extensive research on an individual, call him posing as a legitimate organization he's familiar with, then send a follow-up email that he's expecting and therefore trusts. It's gotten to the point that if a highly skilled hacker wants access, he or she will get it. This is why early detection and rapid response are so important.

QUICK HIT 4

Firms should be prepared for the likelihood that it could happen to them and take steps in advance to limit the potential damage. This might involve purchasing specialty insurance or seeking help from outside consultants. But above all, it means having a plan in place.

Most organizations — not just law firms — have a long way to go on this count. Recent statistics suggest that the median breach goes undetected for more than 200 days, and most organizations learn they've been breached from outside sources (such as law enforcement or security researchers).

Firms should be prepared for the likelihood that it could happen to them and take steps in advance to limit the potential damage. This might involve purchasing specialty insurance or seeking help from outside consultants. But above all, it means having a plan in place.

When a breach is discovered, it will trigger a slew of hard decisions that may affect the continuity of operations. In addition, there will be the delicate task of notifying clients and, perhaps, firm employees. In fact, almost all states now have security breach notification laws, as do several federal agencies. As with the firm's disaster recovery and business continuity plans, the cyber breach response plan should be tested and practiced using different breach scenarios.

The senior management of the law firm should send a strong message to lawyers and staff that this is a critical and hugely important role of everyone in the firm. Further, management should not rely solely on the systems personnel to "take care of this." Some level of outside, expert assistance is recommended, if only to periodically test or audit the vulnerability of the system. Because the detection and especially the forensic analysis and assessment of the breach is vital, outside help may be required there also.

QUICK HIT 5

The senior management of the law firm should send a strong message to lawyers and staff that this is a critical and hugely important role of everyone in the firm.

"Properly addressing the threat requires a tremendous investment of time and resources across the firm — it doesn't happen overnight, and it never ends," notes the representative from the international AmLaw firm. "Firms tend to underestimate what it truly takes to prepare, plan, and remediate systems and security programs, then underappreciate the effort needed for ongoing monitoring, maintenance and education.

"[It] really requires a change in attitude, and ultimately culture, across the entire organization where security is concerned. That is the only way it becomes a priority and the proper investment is appreciated and made. Bottom line, security is inconvenient, and firms just have to accept that fact and make addressing it a priority if they have any hope at being successful in protecting themselves and, most importantly, their clients."

Senior management, send a message to your firm — and ultimately to your clients — that your firm will do everything reasonably possible to prevent, detect and respond quickly to a breach in the security of your information systems. You cannot afford to wait any longer. Act now.

QUICK HIT 6

It's gotten to the point that if a highly skilled hacker wants access, he or she will get it. This is why early detection and rapid response are so important.

ABOUT THE AUTHORS

Jack M. Vaughan is the former Administrative Partner at Fulbright & Jaworski (now Norton Rose Fulbright), having retired in January 2013 after 27 years in that position. He now consults with law firms on risk management issues and is an adviser to Control Risks, an international risk consultancy.

Email

Eben Kaplan is a Senior Consultant at Control Risks, where he focuses on cybersecurity. He has a master's degree in cybersecurity and previously worked as an analyst for the Department of Homeland Security.

Email
Website