

# The **role of governance** in cyber security

BY IAN RAINE

To read the entire issue of  
**Legal IT Today** [click here](#)



Law firms are particularly attractive targets for cyber criminals. They need to rethink how they protect client data.

In the legal industry, reputation is everything. Clients want to believe you are the best at what you do and that they can trust you during their most vulnerable times. So what if someone were to ask you as a legal professional: 'What is the biggest threat to the public reputation of your firm and your clients today?'

How would you answer them? Would it be your firm's win-loss record, the growing competitiveness of the industry or something similar? While these are natural first responses, the reality is that the biggest threat facing the legal industry today is cyber security.

All it takes is one click on your favorite news site or one glance at the TV to confirm that this is the case. From the Panama Papers to the 'Oleras' BigLaw breaches, the news is full of stories relating to cyber security attacks on legal and other professional services firms – and the trend is showing no sign of slowing down. As an industry, we must take action to get ahead of these criminals. Law firms of all sizes must go beyond preventative perimeter security and put processes in place that are designed to mitigate the effect of attacks that breach the perimeter security.

Even if having a conversation about these processes is not prompted by a breach of your own system, it stands to reason that with the prevalence of hacks, clients will soon be demanding to see how you govern their information and how you are prepared to mitigate risk. It will be up to individual law firms to demonstrate this preparedness before risking losing business. In order to arm yourself against potential hackers, it is important first to understand the frequency with which law firms are being attacked, how they are attacked, and why they are being targeted in the first place.

According to the American Bar Association, 25% of law firms with 100 attorneys or more have experienced a security breach of some type or another. When not controlling for size, other reports estimate this figure to be as much as 97% of firms. Of these attacks, 25% were the result of malicious activity

---

*As cyber criminals become more sophisticated, governance will be key to preventing breaches*

---

within the company and 80% were a result of stolen credentials from a phishing attack.

Phishing, by far the most popular choice for hackers looking to gain inside access to firm information, comes in many forms. There is the traditional method, which involves casting a wide net to thousands of email addresses without targeting anyone in particular. Then there is spear phishing, where attackers research their targets using the wealth of information on the web and send highly targeted and custom emails to a small number of individuals in a single firm or a single department of a firm. M&A firms are common targets here. And finally there is whaling, which refers to the spear phishing of high-level executives who are likely to have access to the most valuable information.

Phishing threats are significant and must be taken into account when reviewing current security measures across the organization.

Why are law firms taking the brunt of the cyber security blow when it is not their own data but their clients' data being hunted? The answer is twofold. First, a single firm can serve as the access point to the data of hundreds of clients. Second, standards of security at law firms are often not as stringent as those of many of their high-profile clients. You may have heard law firms described as the 'soft underbelly' of corporations, and it is often true. Law firms – especially smaller and midsize ones – simply do not have the same level of security.

As a result, more corporate clients are demanding their law firms take increased security measures, often

through demanding Outside Counsel Guidelines that lay out how information will be stored and protected. Additionally, clients are exercising their right to perform security audits on their law firms to check that appropriate measures are in place.

To meet these growing expectations, many organizations are spending the majority of their security budget protecting their network against the emerging threats of the Internet. They're purchasing expensive firewalls, intrusion detection and prevention systems to help mitigate these malicious activities.

The overriding emphasis is on prevention and detection – alerting firms to when a breach has occurred, what steps to take to address the breach and how quickly those steps need to be taken. However, there is another, often overlooked, layer of security that should be part of any law firm's cyber protection; one that assumes some level of the perimeter has already failed without your knowledge. This layer is governance.

Governance includes your firm's ability to associate every piece of client data with a specific policy. If policies are comprehensive, they will dictate where information is saved, what other information is saved with it, how long it is stored in that location (physical or digital) and who has access to it.

Governance is the opposite of the world of free and open internal access that many of today's professional service firms are operating in. Governance also includes the ability to encrypt content both at rest and in motion – ensuring a rogue user with admin credentials cannot view content contained in a central document store or tap information as it's sent around the firm—as well as tracking what has happened and which documents a user has accessed through an effective audit trail.

This kind of 'pessimistic' security model may feel uncomfortable or stifling at first, but it is critical to allowing only those individuals who are members of a particular matter team to access sensitive client data. It also protects clients by making sure that if a user's credentials are compromised, a hacker's impact is limited only to what that account has access to.

To say it another way, a hacker can't steal what they can't see. And as cyber criminals become more sophisticated, governance will be key to preventing breaches. According to a recent ILTA technology survey, the number of firms moving to a pessimistic security model has increased by 50% over the past few years. This will continue to rise, and the future of the legal industry's reputation depends on it.

*Ian Raine is director of product management at iManage. ■*

