CYBERSECURITY LAW & STRATEGY

NOVEMBER 2019

Safeguarding Your Intellectual Property

By Matthew Calcagno

Documents are the lifeblood of any law firm. The documents that a firm produces are its greatest asset, yet firms historically have not made sufficient efforts to safeguard those documents from both internal and external threats.

For decades following the advent of word processing systems and continuing even into today's sophisticated document management platforms, law firms have typically had an open-door approach to document access. This means that anyone in your firm can likely access any document at any time, leaving your firm's intellectual property entirely unprotected.

With law firms featuring prominently in headline stories about cyberattacks and security breaches, the old way of doing things no longer works. Changes to document management and security have been long overdue, and the time to start implementing new procedures is now. The open-door practices of the 1990s need to be brought into the 21st century by implementing need-to-know policies that offer the security required in the present day.

Closing the Open Door

Law firm documents have always been susceptible to security threats, even before the sophisticated cyberattacks that we see today. Firms have faced an everyday threat of users losing data or documents being stolen, either by internal or external thieves. In the past, law firm document systems were not really set up with protecting documents as one of their primary goals.

In large part, this is because systems were typically designed with user convenience as the main priority. Document protection and user convenience are often at odds when it comes to day-to-day operations — lawyers want to be able to access any document they want to see at any time, but allowing that level of openness leaves documents entirely unprotected and creates the perfect conditions for a security breach. Placing restrictions on document access

necessarily reduces the level of unfettered convenience that lawyers have enjoyed in the past, and for that reason firms have been loath to implement such procedures.

In addition to the convenience factor, law firms historically also simply gave little thought to protecting their documents from internal users. It has only been since the rise of external security threats that firms have started focusing more attention on these issues and are now looking to institute safeguards against both internal and external breaches.

Document Security for Modern Times

Overcoming the convenience issue starts with getting users to understand the threat, particularly lawyers or partners who have been at the firm for decades and are used to the way things have always been done. If your users understand that the threat at hand is being the next front-page story, they'll be more likely to get on board with new security procedures that will actually safeguard the firm's intellectual property.

Law firm users now access documents in very different ways than in the past, when lawyers worked entirely from desktop computers in their offices. Today's lawyers are constantly on the go, opening documents in the document management system from mobile devices and through mobile applications. While your framework may be set up for security, you're still relying on user credentials that can easily be stolen and your old system won't ever offer your documents complete protection.

If a single one of your users gets hacked, that hacker gains access to millions of documents through open-door policies. In contrast, if you establish a zero-trust network to protect your documents and give your users access to only those documents that they need to see, you have significantly greater protection in the event that credentials are compromised and your system is breached.

Switching over to a need-to-know document access policy can take significant work, but the potential risk is too great not to do it. Firms face internal and external threats all the time — from disgruntled employees to entire practice groups moving to a competitor. In those scenarios, there may be no way to protect the documents those individuals had access to, but if you've implemented procedures that protect the intellectual property of other practice groups, that will go a long way toward protecting your firm.

Your documents and your document management are your firm's greatest assets. It's time to institute updated procedures to safeguard them.

The Way Forward

If you haven't seriously started thinking about your document management procedures and your document security, the time to start is now. Even if you have thought about it, if you're like many firms, you may be hesitating to take action because this is new territory. Most firms have not addressed a change like this before, and it can be daunting to put a plan together.

The good news is that there are solutions available on the market that can make it easier to implement need-to-know access, as well as experienced vendors who can make the

transition easier. For example, iManage, one of the most popular document management systems in the legal industry, offers a product that makes the transition to need-to-know access much simpler for its clients. The iManage Security Policy Manager allows you to implement need-to-know access for documents on a global scale, segregating your content and implementing the ethical walls you need to maintain security in the face of today's looming threats.

These kinds of solutions allow you to protect your documents without sacrificing your performance or productivity. While the unfettered convenience of the past may not be there, your employees will still be able to get to anything and everything they actually need to see to do their jobs. Need-to-know access can easily be set up on client-, project- or matter-centric bases, providing the necessary security without impacting your firm's resources or systems.

When you segment your document system and restrict access on a need-to-know basis, you greatly minimize the impact of any potential cyberattack or security breach. Employee credentials can only be used, either by that employee or someone who improperly obtains those credentials, to access the specific documents for which that employee has permission. This means that any breach is contained and your entire system is no longer at risk.

Regardless of the document management system you currently use, similar measures can be put in place to ensure that your documents are secure. An experienced IT vendor can help you analyze your security framework and implement the right solutions that work with your systems and preferences.

Most law firms handle thousands of matters, which produce hundreds of thousands of documents to manage. The sheer volume of documents at issue can make changing the way those documents are managed feel like a daunting task. However daunting it may be, though, it isn't impossible. Today's technology makes it easier to assign groups to massive workspaces and institute a need-to-know framework. The key to getting started is to get the right help so you can truly understand how to tackle the problem. With the right education, the solution can be a lot easier than you might think.

The solution to modern document management and security lies in addressing access in terms of groups. The ability to use groups to structure document management has existed for years, but too many firms have declined to implement it simply out of fear of inconveniencing their users. With today's significant threats to document security, there's no longer time to wait.

The Future of Document Management Is Need-to-Know

Need-to-know access is the only way to truly secure your sensitive law firm data in today's technological age. By restricting document access to certain clients, projects or teams, you can be sure that your employees are only getting to the documents and data they truly need to do their jobs and are not capable of compromising your entire system.

Today's technologies are flexible enough to allow you to configure your need-to-know access in ways that still allow you optimal performance while creating minimal interruptions to your daily workflows. While any change will inevitably put some burden on your IT staff as employees struggle to adjust to the new way of doing things, achieving the right balance between convenience and security is crucial going forward.

Until now, that balance has been too far in favor of convenience, opening law firms up to the possibility of major, unrecoverable breaches. This overriding desire to not inconvenience has led firms to not address the very real risks they're facing.

No one wants to be the next big breach headline. By implementing need-to-know access for your documents and data, you'll be well on your way to mitigating cyberattacks and securing your critical intellectual property from both internal and external threats.

*****

Matthew Calcagno is an Information Security Consultant at Keno Kozie Associates (www.kenokozie.com). He has two decades of document management experience and has a passion for improving the overall security landscape of a company. Matthew received his Bachelors of Business Administration in Computer Science at Robert Morris University and did his Graduate studies at Eastern Illinois University.
