LEGAL workspace
Your Law Office in the Cloud

How to win outside counsel for an INSURANCE GIANT

Learn what Fortune 500 companies look for when selecting outside counsel.

LEGAL workspace
Your Law Office in the Cloud

Winning Large Clients

When your firm handles insurance defense, you receive, send, and store highly sensitive materials. Wise law firms understand that security and compliance are critical because of the growing threat to cybersecurity. Without the proper safeguards in place, you put clients' information at risk and jeopardize your reputation. And large insurance companies simply won't hire you if you don't apply the right controls and protocols to keep their data safe.

They're right to be cautious: 80% of the largest 100 law firms have been hacked since 2011, according to the American Bar Association in 2015. Law firms are a prime target for hackers because they store large amounts of high-value, confidential data. In "The Security Vulnerabilities Law Firm Hacks Create for Corporations," which appeared in Inside Counsel in June of this year, Amanda Ciccatelli writes, "IT capability is often viewed as an administrative function, not an integrated business capability, and as a result, information security has suffered."

The rewards of working with large corporate clients are sizeable. To get your foot in the door, you need to be aware of vulnerabilities, be able to bolster security, and meet insurance companies' compliance requirements.

There are ways to determine what holes you have in your security controls and how to patch them. You should, for example:

1. Protect and back up data and plan for recovery

Data encryption, dual-authentication, administrative policies, firewalls, and intrusion detection systems can help protect data. Secure off-site back-ups are another key component to data security. If a breach still occurs, know how you'll respond—and how quickly you can be back up and running. The American Bar Association article, "Facing the Cybersecurity Threat to Your Firm," experts say that "[a]dvance planning is critical for effectively responding to a data breach, and that includes an incident response plan."

2. Perform a tech review and assessment

Since new cyberthreats emerge regularly, you should routinely assess and patch your vulnerabilities. Pay attention to audit logs, so you know who accesses what files and can see if something unusual happens.

3. Understand what devices attorneys and other staff use to work.

Are they using their personal Smartphones and laptops to work outside the office? Are they carrying client information on flash drives? What kinds of safeguards are in place on those devices?

4. Control access to information

If an attorney isn't working on a particular case, there's no reason for him/her to have access to it. This precaution isn't about attorney ethics—client confidentiality is paramount to lawyers. Rather, it's about decreasing the number of ways that hackers can access information. Train employees and attorneys to follow security protocols. As Chris Pogue, CISO of Nuix Solutions writes, "Protecting your information is a battle that is fought by every member of your organization, from the most senior partner to the newest intern, who has access to any data of value."

These recommendations can be used by law firms looking to increase security in order to be more attractive to any large corporation, but there are also "insurance-specific uses of technology, internal and external research capabilities, and client support databases that should be a part of a law firm's technology resources," according to an article written by Bob Dolinsky, CIO of Sutherland Asbill & Brennan.

Crafting a strategy and executing its steps may seem like expensive, time-consuming, and technical work. But it all depends on the avenue you take. Working with an IT firm on a project like this can end up costing tens of thousands of dollars, and the process can last months.

6. Faster and Less Expensive Solution

Legal Workspace can take a project like this off your hands and deliver it more quickly than you might expect. Depending on the size of your firm, it could take only a week for Legal Workspace to perform a cybersecurity audit and apply the appropriate controls for compliance with large insurance companies' standards and with government regulations.

And, if you're considering getting into the insurance defense game, but you're concerned about the upfront costs of upgrading your IT to handle compliance requirements, Legal Workspace's fees are only a fraction of the cost of working with an IT firm.

The other upshot of selecting Legal Workspace to help you get compliant is that as new threats emerge and security standards evolve, you don't need to worry about shelling out more money: Maintenance and updates are automatically included.

There are usually a lot of hurdles a law firm has to jump in order to win the business of a large insurance company. The security and compliance hurdle doesn't have to be the most difficult and expensive one to clear.

Legal Workspace is a pioneer in cloud-based work environments and data storage designed specifically for law firms. Learn more at legal-workspace.com.