7 Urgent Security Protections Every Law Firm Should Have In Place Now

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium law firms who are "low hanging fruit." Don't be their next victim! This report will get you started in protecting everything you've worked so hard to build.

SpliceNet

Provided By: SpliceNet Legal Tech
Author: James Gast & David Myers
9624 Cincinnati Columbus Rd.
Suite 203, Cincinnati, OH 45241
jgast@splice.net | 513.252.0212
www.splice.net

Are You A Sitting Duck?

You, the Managing Partner. Legal Admin or Office Manager of a law firm, are under attack. Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of law firms like yours to steal credit cards, client information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses.

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot? Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small-medium firms; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

In fact, the National Cyber Security Alliance reports that one in five small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more businesses utilize cloud computing, mobile devices and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these 7 security measures in place.**

1. **Train Employees On Security Best Practices.** The #1 vulnerability for business networks are the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network and firm.

2. **Create An Acceptable Use Policy (AUP) – And Enforce It!** An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the web sites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what web sites your staff access and what they do online during company hours and with company-owned devices, meanwhile giving certain users more "freedom" than others.

   Having this type of policy is particularly important if your staff are using their own personal devices to access company e-mail and data.

If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, it can be a gateway for a hacker to enter YOUR network. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

Furthermore, the data in your law firm is much more highly sensitive, client confidential data such as patient records, credit card information, financial information and the like, potentially you are not ethically permitted to allow employees to access it on devices that are not secured; but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

3. **Require STRONG passwords and passcodes to lock mobile devices.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

4. **Keep Your Network Up-To-Date.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

5. **Have An Excellent Backup.** This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be automated, monitored and TESTED; the worst time to test your backup is when you desperately need it to work!

6. **Don't allow staff to download unauthorized software or files.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps. This can largely be prevented with a good firewall and staff training and monitoring.

7. **Don't Scrimp On A Good Firewall.** A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT person or company as part of their regular, routine maintenance.

Want Help In Implementing These 7 Essentials?

If you are concerned about staff and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

At no cost or obligation, we'll come to your office to conduct a free **Law Firm Security And Backup Assessment** of your firm's overall network health to review and validate as many as 60 different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free assessment, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?

- Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).

- Are your staff freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?

- Are you accidentally violating any PCI, HIPAA or your Ethical Responsibilities? New laws and Ethical Opinions are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines. **Note this will not be legal advice.

- Is your firewall and antivirus configured properly and up-to-date?

- Are your staff storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the 100's of firms we've worked with over the years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Law Firm Security And Backup Assessment**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at 513.252.0212 or you can e-mail me personally at jgast@splice.net

Dedicated to serving you,

James R. Gast, Jr
Web: www.splice.net
E-mail: jgast@splice.net

Here's What A Few Of Our Clients Have Said:

"Area's ONLY Expert."

If Jim has something to say about Legal IT, you should listen! Jim and his team has worked with Law Firms and Technology for nearly 20 years and is the area's ONLY Expert (or at least the only one I'd trust). I've trusted Jim and SpliceNet for the last 15 years to manage our firm's technology and keep our data secure. More recently SpliceNet implemented our On-premise Cloud Servers and a Disaster Recovery environment and virtually eliminated our downtime and improved our firm's bottom line by keeping our staff working. I sleep better at night knowing that SpliceNet has things under control.

Mark E. Godbey, Esq., Owner
Mark E. Godbey & Associates

"Wow, what a difference in service!"

"I'm SO glad we hired SpliceNet. Wow, what a difference in service! Now our computers work the way they're supposed to and we aren't constantly plagued by frustrating problems. I highly recommend you call SpliceNet today!"

Erik Crew, Communications Manager
Ohio Justice and Policy Center

"SpliceNet takes ownership of my problems."

The team at SpliceNet is personable, professional and understands my priorities. They are always willing to answer my questions and use plain English rather than "tech speak". SpliceNet takes ownership of my problems, persistently pursues a solution and It gets done right the first time without any surprises charges. We are extremely satisfied with them and in my book SpliceNet is a 10!

Nan W., Office Administrator
Schwartz Manes Ruby & Slovin