NetworkTitan

The 7 Most Critical IT Security Protections Every Law Firm Must Have In Place NOW To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

Cybercrime is so widespread now that it's practically inevitable that your firm – large or small – will be attacked. A few small preventative measures, however, CAN PREPARE YOU and minimize (or outright eliminate) any reputational damages, losses, embarrassment and associated costs.

Cybersecurity & IT Service Professionals

Provided By: Network Titan
Author: Mike Hughes
www.networktitan.com
619-255-2621

NetworkTitan

"Not My Firm… Not My People…" You Say?

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot? Or that you have "good" people and protections in place? THINK AGAIN. 2020 broke all records when it came to data lost in breaches and sheer numbers of cyber-attacks on companies, government, and individuals. Infosecurity Magazine reported that 'a new organization became a victim of ransomware every 10 seconds in 2020 with remote workers experiencing a sharp uptick in threats' and almost HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR and out of sheer embarrassment – but make no mistake: small businesses are being compromised daily, and the smug ignorance of "that won't happen to me" is a surefire way to leave yourself open to these attacks.

Our digital landscape is changing. Botnets, malware and brute force attacks all thrive in our "work from anywhere" environments. Phishing, smishing and vishing are all gaining traction on multiple platforms.

You hear about it daily or see it on the news - the latest data breach, software vulnerability or ransomware attack. Cybercrime is growing exponentially. **Because of all of this, it's critical that you have these seven security measures in place.**

"But my IT is great, I trust them…"

Many firms are shocked when they get compromised because they BELIEVED their IT people had it "handled." However, there is a virtual army of thousands of hackers and very sophisticated crime rings that work around the clock to overcome <u>known</u> protections – and you can't stop a brand-new threat that was invented yesterday with a security system that was designed six months to a year ago. It requires special expertise to stay on top of all of this, which is why many don't.

To that end, here's your quick 7-step checklist. If your firm isn't actually implementing ALL of these protocols – OR if you don't know if you are – WHY NOT? <u>What hasn't your current IT company told you about all of this</u>?

1. **The #1 Security Threat To ANY Law Firm Is**… ***You!*** Like it or not, most security breaches in business are due to an employee clicking, downloading or opening a file that's infected, either from a website, e-mail or text; once a hacker gains entry, they can infect other devices on the network. Phishing e-mails (an e-

mail cleverly designed to look like a legitimate e-mail from a website or vendor you trust) have evolved. They are more authentic looking and more difficult to detect than ever before, and they are still ***very*** common – spam filtering and antivirus cannot protect you if someone is clicking on and downloading something malicious. That's why it's CRITICAL that you educate your entire staff on how to identify an infected e-mail, smishing or vishing scam. Cybercriminals are EXTREMELY clever and can dupe even sophisticated users. All it takes is one slip up.

On that same theme, the next precaution is implementing an Acceptable Use Policy. 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. We can easily set up permissions and rules that will regulate online access, giving certain users more "freedom" than others.

Having this type of policy is particularly important if employees are (and everyone is) using their own personal devices and home wi-fi to access company e-mail and data. With staffers accessing so many cloud apps, you are considerably exposed. An infected or unprotected, unmonitored device can be a gateway for hackers to gain access – which is why we don't recommend you allow employees to work with unprotected personal devices.

Consider this; if an employee leaves, are you allowed to erase company data from their phone or personal laptop? If their phone or computer is lost or stolen, are you permitted to remotely wipe it – which would delete all their files, photos, videos, texts, etc. – to ensure your firm and client data isn't compromised? An AUP addresses these important and often overlooked policies.

2. **Require STRONG passwords and passcodes to lock mobile devices.** Now it's recommended that they are longer than 8 characters – think phrases – that are long but easy to remember. On a cell phone, requiring a passcode to be entered goes a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't choose easy-to-guess passwords, putting your firm at risk. Are they? If everyone in your firm is not being forced to do a password reset every 30-60 days, ***your IT is failing you***.

3. **Keep your network and all devices patched and up-to-date.** New vulnerabilities are frequently found in the common software programs you are

using, therefore, it's critical you patch and update your applications and systems when patches become available. If you're under a managed IT plan, this can be automated for you so you don't have to worry about a connected device missing an important update.

4. **Have A Business-Class Image Backup BOTH On-Premise and In the Cloud.** 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 properly backed up, you don't have to pay a crook to get them back. A good backup will also protect you against accidentally (or intentionally!) deleting or overwriting files, and against natural disasters, water or food damage, fire, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it!

5. **Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT department.** The use of personal and mobile devices in the workplace has exploded. It's now easy to gain access to pretty much any type of company data remotely; all it takes is a known username and password.

   But this has drastically increased the complexity of keeping a network – and your firm's data – secure. In fact, one of the biggest dangers now is that one of you will log in to your network via a personal device that is infected, thereby giving a hacker easy access – an open doorway to all of your critical data.

   Today you need to make sure all personal devices are properly secured, monitored and maintained by a security professional. One of the fastest ways cybercriminals access networks is by duping unsuspecting users into willfully downloading malicious software by embedding it within downloadable files, games or other "innocent" looking apps.

   But here's the rub: most employees won't want you monitoring and policing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your firm.

6. **A Business-Class Firewall and Proper Updates.** A firewall acts as a frontline defense against hackers, blocking everything you haven't specifically allowed to enter (or leave) your computer network. All firewalls are not created equal and all

need monitoring and maintenance, just like all devices on your network do, or they are completely useless. This too should be done by your IT person or company as part of their regular, routine maintenance. HOWEVER, it's not uncommon for IT to configure intrusion detection and prevention features incorrectly; often they are disabled during a project, and never turned back on, making the tool useless.

7. **Protect Your Bank Account.** Did you know your firm's bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. (Don't believe me? Go ask your bank). Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, NOT fraud.

   So here are 3 things you can now do to protect your bank account:

   a. Set up e-mail alerts on your account so you are notified any time money is withdrawn. The FASTER you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the DAY it happens can be stopped.

   b. Dedicate ONE computer for online banking and never access social media sites, free e-mail accounts (like Hotmail) and other apps like games, news sites, etc., with that computer. Remove all bloatware (free programs like MS Silverlight, Adobe and offers from the device manufacturer, etc.) and make sure that device is monitored and maintained behind a strong firewall with up-to-date security protections.

   c. Finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account.

   All of these things will greatly improve the security of your accounts.

Are You REALLY Willing To Be Complacent About This?

Look, I know all of this appears to be a giant distraction and cost that interferes with REAL work. You and I both realize that implementing proper security protocols won't win you the "Lawyer of the Year" award but….

NetworkTitan

Mark Twain Once Said,

"Supposing Is Good, But KNOWING Is Better"

If you want to know for SURE that your current IT company (or IT person) is truly doing everything they can to secure your network and protect you from ransomware, bank fraud, stolen and lost data and all the other booming cyber threats along with the problems and costs associated with them, then call us for a **FREE Cyber Security Risk Assessment**.

At no cost or obligation, we'll conduct a **Cyber Security Risk Assessment & Dark Web Scan** of your firm's overall network health and domain to review and validate data-loss and security loopholes and vulnerabilities. We'll also look for common places where security and backups get overlooked. You will know where your firm stands.

At the end of this free assessment, you'll know:

- Are you 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 – and (more importantly) how FAST could you get your IT systems operational if hit with ransomware? We'll 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 staffers accessing time wasting websites, looking for other jobs, or checking personal email and social media accounts? You know some of this is going on right now, but do you know to what extent? Are they downloading sketchy video and music files exposing your firm to cyber threats?

- Is your security package configured properly and up-to-date? No security protections are "set and forget." They needs to be constantly monitored and updated – is yours? Is your IT department giving you the assurances that it is?

- Are employees storing confidential and important information on unprotected apps like Dropbox that are OUTSIDE of your backup? Could they walk off the job and go to work for a competitor, bringing your confidential data with them?

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 firm is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the hundreds of businesses and firms we've audited 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 third party to validate nothing has lapsed or been 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 Cybersecurity Risk Assessment & Dark Web Scan**. 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.

Get the facts and be certain your firm, your reputation and your data are protected. Call us at **619-255-2621** or you can e-mail me personally at mike@networktitan.com

Dedicated to your security,

Mike Hughes

www.networktitan.com
mike@networktitan.com
619-255-2621