BOOMTECH
WE GET IT DONE!

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

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium Businesses that 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.

Provided by: BoomTech, Inc.
Author: Philipp Baumann
23123 State Road 7, Suite 260
Boca Raton, FL 33428
561-300-5080
www.BoomTechIT.com
pbaumann@BoomTechIT.com

Are You A Sitting Duck?

You, the managing partner of a small to medium sized business, 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 small businesses 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 J.P. Morgan or Home Depot? Think again. 1 million NEW malware threats are being released every single day and 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, lawsuits, data-breach fines = not to mention, sheer embarrassment.

In fact, the National Cyber Security Alliance reports that one in five small businesses have been victims of cyber-crime in the last year — and that number is growing rapidly as more businesses utilize cloud computing and 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. **The #1 Security Threat To ANY Business Is... You!** Like it or not, almost all business world security breaches are due to an employee clicking, downloading or opening a file that's infected, either on a website or in an e-mail; once a hacker gains entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (e-mails cleverly designed to look like legitimate messages from a web site or vendor you trust) is still a very common occurrence — and spam filtering and anti-virus software cannot protect your network if an employee is clicking on and downloading the virus. That's why it's CRITICAL that you educate all of your employees on how to spot an infected e-mail or online scam. Cybercriminals are EXTREMELY clever and can dupe even sophisticated computer users. All it takes is one slip-up, which is why constantly reminding and educating your employees is critical.

   On that same theme, the next precaution is implementing an Acceptable Use Policy (AUP). 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. Furthermore, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what websites your employees access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

   Having this type of policy is particularly important if your employees are using their own personal devices and home computers to access company e-mail and data. With so many applications in the cloud, an employee can access a critical app from any device with a browser, which exposes you considerably.

   If an employee is logging into critical company cloud apps through an infected or unprotected, unmonitored device, it can be a gateway for a hacker to enter YOUR network — which is why we don't recommend that you allow employees to work remotely or from home via their own personal devices.

   Second, if that employee leaves, are you allowed to erase company data from their phone or personal laptop? 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, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally 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 and cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

2. **Implement The CIS 20 Critical Security Controls.** The Center for Internet Security provides the 20 Controls each business or small business should have in place. You need to align your business to those each quarter to ensure you are doing everything possible to protect your clients' data. This includes having proper inventory of your hardware and software, implementing data recovery capabilities in case you fall victim to a cyber-attack and more - click on the link below for the full list. https://www.cisecurity.org/controls/-cis-controls-list/.

3. **Security Assessment. Data Breach Liability Report. Quarterly scans.** Complexity is the enemy of security. A combination of scanning technology with advanced analytics makes for an ideal single go-to solution.

How Does It Work?

Step 1: Triple-Threat Detection
The first step is to discover the unprotected data on a network, along with vulnerabilities and access permissions.

Step 2: Data Breach Liability Report
Each quarter we will review the potential risk and cost associated with that risk in the event of a data breach.

Step 3: Risk Review
After discovering the risk, we can now analyze and see if we can eliminate the risk. For example, often files are getting saved to the network that don't need to be. If we establish that we need to keep the files, we can setup proper mission and security procedures as well as drive encryption to protect that data.

4. **Deploy a Next Generation Endpoint Protection.** Next-generation endpoint and server protection uses several layers of attack prevention, including behavior detection and machine learning, to stop attacks that other vendors simply can't. It also provides unparalleled threat visibility at a minimum system impact. BoomTech recommends Webroot.

5. **Setup Two-factor authentication (2FA) for any possible log in.** 2FA is a second layer of security to confirm a user's claimed identity by using something they know (password) and a second factor other than something they have or something they are. An example of a second step is the user repeating back something that was sent to them through an out-of-band mechanism (such as a code sent over SMS), or a number generated by an app that is common to the user and the authentication system. By enabling 2FA even if your username and password get compromised, the hacker still cannot log into your account. Ensure all your online accounts such as E-mail M365, Gmail and any banking accounts are protected by 2FA again the more the better. Popular 2FA apps such as Authy https://authy.com/or Google authenticator allow you to have all 2FA codes under one app.

6. **Protect Your Bank Account.** Did you know your company'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 what their policy is on refunding money stolen from your account!) 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 do to protect your bank account. First, 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 on the DAY it happens can be stopped. If you discover even 24 hours after it's happened, you may be out of luck. That's why it's critical that you monitor your account on a daily basis and contact the bank IMMEDIATELY if you see any suspicious activity.

   Second, Require YOUR signature and 2 factor authentications for any wire transfers. Also set a written wire transfer policy for all employees that if wire instructions get changed via e-mail, they are to pick up the phone and call the bank to verify it came from them and not a hacker.

   And finally, contact your bank and shut down any debit cards associated with that account. All of these steps will greatly improve the security of your accounts.

7. **Keep your network and all devices patched and up to date.** New vulnerabilities are frequently found in common software programs you are using, like Windows operating systems. I hope you are no longer using Windows 7, which reached end of life as of 1/14/2020 this year. You also have to patch your 3rd party applications such as Adobe, Flash or QuickTime; therefore, it's critical that you patch and update your systems and applications when one becomes available. 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.