How Small Businesses Can Safeguard Against Cyber Attacks

By: Jamshid Javidi, President of CEO Computers

Let's get straight to it – cyberattacks against small businesses are on the rise. We've all seen news reports about large companies being hacked, customer information being leaked, and worst-case scenarios related to Ransomware. However, that doesn't leave smaller businesses safe from these threats or their costly aftermath.

Terms such as: Key loggers, spam, ransomware, root kits, Trojans, spyware, worms, viruses, adware, and scareware have become familiar and regularly used on a daily basis. Each of these threats comes with different payload and delivery method. Just one solution such as antivirus or malware will not be enough to defend your network and precious data.

For the past 30 years, we here at CEO Computers have seen and heard it all and experienced these malicious attacks firsthand and assisted victims of these attacks throughout their difficult recovery.

We've put together a summarized list of the top 17 ways you can safeguard your small business and keep the cyber-attacks against your company at bay. These are brief tips and not in any particular order, but of equal importance. We recommend that all to be implemented equally to provide an effective protection for your business.

1. **Develop protocol & policies that keep your data safe--** Create rules and protocols for every employee to follow. According to IBM, 85% of cyberattacks are unknowingly started by a clueless employee who clicks a suspicious link (such as a pop-up) or provides information over a non-secure network. This makes your employees the weakest link in terms of your overall Cyber Security defense. It is imperative to have regular cyber security training for all of your employees and if required for outside vendors or anyone that might have access to your network.

Perhaps an internal policy that prohibits personal use (checking emails or social media) when on the clock. Also restricting employees from connecting their smart phones or tablets to the company Wi-Fi, downloading freeware software and songs are smart ways to prevent a breach. Included should be policies for BYOD (bring your own device) and accessing your network from outside the office.

2. **Guard your business like a fortress--** Sounds silly, but putting security measures into place can help keep your network safe and secure. A strong perimeter is the basis of a solid security framework that controls access to critical hardware such as your server(s), applications, services and data. Keep the servers, routers, switches not physically accessible to the unauthorized personnel. Preferably all these

equipment should be in an air conditioned room with a security lock. If you do not have a server room it is prudent to purchase a rack cabinet with a lock. If possible monitor the room via a security camera. This way you minimize theft and vandalism.

3. Data Encryption- It is important to identify what is the sensitive data in your network environment (internally and externally) and where is it located and who has access to it. Once these questions are answered you have to make sure the data is encrypted. Microsoft offers Bit locker (encryption software) which is included in Windows 10 Operating System. For Network Server there are other programs are available as well.

4. **Email Encryption**- Any sensitive data that is transmitted via email should be encrypted. Microsoft offers email Encryption program as well as there are many third party software that offer email encryption.

5. Password Policy-- Always implement very strong network passwords (known as complex passwords with 8 or more characters including upper and lower case letters as well as special characters !@#$) and change them regularly (recommended every 90 days). It is important to have passwords for logging in to your network, accessing your email, and applications. Also, DO not use the same password for all of your accounts.

6. Wi-Fi usage and policy-- Make sure your Wi-Fi uses a different subnet IP than your network, has a strong and a different password. Give the password for the Wi-Fi Network very sparingly.

7. **Stop the negligence—** as mentioned in no. 2 Make sure your server (s) are locked and inaccessible by unauthorized personnel. Make sure that employees are locking their computers when away from their desks. This also can be achieved by implementing screen savers. Make sure that fax machines and printers do not have printouts with sensitive data sitting on them for hours. Passwords are not shared or written on a piece of paper in plain view. Unfortunately, information leaks or stolen data doesn't always come from an outside sources. Do not bring flash drives to the office and connect them to your network.

8. When "Anti" becomes a positive-- Enabling your network with comprehensive yet affordable Anti-Malware or Anti-Virus software is a key component to keeping your systems safe and secure. Malware attacks are on a consistent rise and can impair your computer and network in numerous ways. These attacks are initiated via: Viruses, Spyware, Trojans, Adware and Ransomware. Reputable Antivirus with the latest definitions and updates should be employed and centralized to push the latest antivirus to each node in to your network.

9. Remote Access- It is a norm these days that many employees work from home or outside of the office and some bring their own devices (BYOD) to connect to the server or their local workstations. It is important to follow best standard practices. Make sure there are no open ports that can be exploited form outside. Make sure that remote devices have latest antivirus and are updated. For any remote connections use secure channels such as VPN (virtual Private Networks) and SSL (Secure socket Layer).

10- Utilizing the latest technologies -- It is vital to have a reputable firewall/router that is updated with the latest firmware updates regularly. There are hardware and software products that monitor the traffic on your network and look for suspicious activities. Nowadays, these services are very affordable and offer subscription-based plans – some with no contractual obligations.

11. Backup & Disaster Recovery— When it comes to protecting your data and combatting cyber threats, a reliable backup is the first line of defense, especially online backup with snapshot features in 15-minute increments. With this, if your data is comprised, then you have a recourse. It is highly recommended to backup on different media and keep a copy of the latest backup off the premises. Most importantly, you must verify the integrity of the backup by restoring and testing the backed up data. Most backup programs have an encryption option that should be selected.

12. **Patch Management** & **Remote monitoring and managing (RMM) —** Monitoring and managing your network and connected nodes is another important element of protecting your network, securing your valuable data and achieving minimum requirements of compliance policies such as HIPAA.

This service ensures that all the software patches and updates for the operating systems and third-party software installed on the covered nodes are applied on a regular basis. The RMM agents also check on the health and functionality of the covered computers and servers and report problems and some cases apply remedies to minimize any downtime. It is programmed to reboot the device after any updates.

13. Social Engineering- A majority of cyber criminals spread malware by exploiting a person's trust usually by masquerading as a friend, bank teller, or a manager – and persuading them to click on a link, reveal login credentials, or download a dangerous file. To prepare your employees for these threats, help them identify the tell-tale signs of an online scam like emails that urge users to click on a link, or pop-up ads that offer free goods if the victim fills out a personal survey. Ultimately, your goal is to teach your staff to develop a healthy skepticism of every link, file attachment, and website they see online.

13. Security training –It is imperative to provide regular employee awareness training - After committing to regular awareness trainings and strict password policies, it's important to make sure that employees have fully absorbed the information. Security training essentially reinforces the best-security-practices you want to see in the workplace. In fact, studies show that susceptibility to threats like phishing emails drop by almost 20% after a company runs tests and simulations.

15. Security drills- You should consider conducting quizzes that test the staff's knowledge on identifying phishing scams, responding to malware attacks, and securing their devices. For more practical tests, create role-playing exercises where employees have to avoid common scams from social engineers. Then evaluate their scores based on their decisions during the exercise.

16. 2 Factor authentications. Is another layer of security. It requires the user to log in after being contacted via an embedded code in the text or phone call or email.

17. Cyber Security insurance- if you become a victim of cyber-attacks, the recovery costs (even if you decide to pay the ransom) are quite substantial. Nowadays, Cyber Security insurance is offered by many insurance companies and may not be a bad idea to be considered as your overall action plan to

combat cyber threats. Also, the requirements to be eligible for the insurance are a great roadmap to eliminate security loop holes as well as mitigate any problems. It pays to go through a drill and assume that your network is compromised, or system is hacked.

If you feel all these steps are overwhelming, let CEO Computers a premier Los Angeles Cyber Security company with over 30 years of experience in helping Southern California based companies provide you with a Free network security audit. This audit will expose the security vulnerabilities that your network might be experiencing and provides you with a detailed report on how to eliminate or mitigate them. It will put your mind at ease and will be a good starting point for your action plan against ongoing Cyber threats.

About Us:

CEO Computers is a Los Angeles IT Support & Cloud Solutions company. For over 31 years, CEO has assisted many small businesses located in the Los Angeles area in various industries to implement compliance policies, to secure their network and protect their data.

Protecting your data and eliminate your network security vulnerabilities are our number one goal. For a free network security analysis call us at 818-501-2281 or visit our website www.ceocomputers.com. Call us at 818-501-2281 or visit our website WWW.CEOComputers.com for a Free Consultation today.