Want 17 Ways to Keep Your Business IT Secure?

Small and midsized businesses today are storing data that's attractive to hackers. And now that larger enterprises have bolstered their cyber defenses, SMBs are prime targets for cybercriminals. To help, we've listed 17 things you can do to keep your business IT secure.

1. Conduct Regular IT Inventory Assessments
Determine how your data is handled and protected. Also, define who has access to your data and under what circumstances. Create a list of the employees, partners or contractors who have access to specific data, under what circumstances, and how those access privileges will be managed and tracked. You must know exactly what data you have, where it's kept, and who has rights to access it.

2. Develop An IT Security Policy
Your policy should begin with a simple statement describing the information you collect about your customers and what you do with it. It should identify and address the use of any Personally Identifiable Information (PII), Personal Health Information (PHI) or Customer Information.

3. Protect Data Collected On The Internet
If you collect information on your website, this must be protected. If a third party collects this data for you, they should fully protect it for you. You must ensure any data you collect is secure.

4. Implement Layers of Security
You should not rely on just one security mechanism to protect sensitive data. If it fails, you have nothing left to protect you.

5. Segment Your Networks With Firewalls

Network segmentation categorizes IT assets and data and restricts access to them. Reduce the number of pathways into and within your networks and implement security protocols on these pathways. Do this to keep hackers from gaining access to all areas of your network.

6. Use Measures To Detect Compromises

Use measures like Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs), and anti-virus software to help you detect IT security events in their early stages. Ask your IT provider about an SOCaaS solution. (Security Operations Center as a Service). It will scan your network traffic using Artificial Intelligence (AI). Then logs of information are reviewed by IT professionals. This provides 24/7 detection and response to security threats.

7. Secure Remote Access With A VPN

A Virtual Private Network (VPN) encrypts data channels so your users can remotely access your IT infrastructure via the Internet. It provides secure remote access for things like files, databases, printers and IT assets that are connected to your network.

8. Employ Role-Based Access Controls With Secure Logins

Limiting your employees' authorization with role-based access controls prevents network intrusions and suspicious activities. Define user permissions based on the access needed for their particular job. For example, your receptionist might not need access to your financial data.

9. Enforce Strong Password Control, Don't Use Default Passwords, and Use Other Access Controls

You and your employees should use unique passwords for different accounts. Hackers use sophisticated software with millions of password combinations to attempt brute force attacks. Make sure your passwords contain at least 8 characters with a combination of letters (uppercase and lowercase), numbers and symbols. Don't use the default passwords that come with hardware. Also, use other access controls like multi-factor authentication that verifies users' identities.

10. Install All Security Patches and Updates

Software developers are diligent about releasing patches for new security threats. Make sure you install them as soon as they're released. If you don't, your IT system will be vulnerable to cyberattacks. If possible, set your systems to update automatically. Auto-updates will prevent you from missing critical updates.

11. Enforce Access Policies on Mobile Devices

With BYOD (Bring Your Own Device) use, mobile devices like smartphones, tablets and laptops present significant security challenges. They can be exposed to external threats, infections and hackers, and when connected to your network, can compromise your IT security.

Establish security policies on the use of mobile devices on your network. They should be password protected so only authorized users can use them. Instruct your employees to only use devices that belong to them and have been protected by your security policies. Ask your IT provider about Mobile Device Management.

12. Secure and Encrypt Your Wireless Connections

Be sure your company Wi-Fi is separate from a guest Wi-Fi or public networks. Your internal wireless network should be restricted to specific users who are provided with unique credentials for access. The credentials should be preset with expiration dates, and new ones provided periodically. Your company's internal wireless should also be protected with WPA2 encryption.

13. Back Up Your Data

You must have a backup copy of your data if it's stolen or accidentally deleted. Develop a policy that specifies what data is backed up, how often it's backed up, where it's stored and who has access to the backups. Backup to both an external drive in your office and a remote, secure, online data center. Set backups to occur automatically. And make sure your backup systems are encrypted.

14. Conduct Cybersecurity Training For Your Employees

When employees aren't aware of security threats, your business IT is vulnerable. Make sure they receive initial and periodic cybersecurity training that includes information on phishing, spear phishing and social engineering attempts that try to trick them into performing actions that will infect your network. In addition to suspicious emails and websites, they should be cautious about phone calls and voicemail alerts from unknown parties.

15. Leadership Must Be A Part Of Cybersecurity

Your business won't be secure if your executives aren't involved in your IT security. Your C-suite executives must also go through cybersecurity training and be aware of existing threats, security incidents and how to prevent them.

16. Develop A Cybersecurity Response Plan

Your plan should include input from all departments that could be affected by a cybersecurity incident. This is a critical component of emergency preparedness and resilience. It should also include instructions for reacting to destructive malware. Departments should be prepared to isolate their networks to protect them if necessary.

17. Plan For Data Loss Or Theft

It's essential that you determine exactly what data or security breach regulations affect your business. You need to know how to respond to data loss. All employees and contractors should be educated on how to report any loss or theft of data, and who to report to. Data loss can expose you to costly state and federal regulations and litigation. You must be able to launch a rapid and coordinated response to a data breach to protect the reputation of your company.

To keep your IT secure, consult a cybersecurity expert like Network Outsource. We have the tools and knowledge to protect your business from any threat.