SECURITY TECH-CHECK: FAQ

What if my business is in the cloud?
All of the sections above are relevant for you, even if you manage your IT in the cloud. Cloud solutions vary in how they implement security. Sometimes it is built in, but just as often you need to purchase or enable add-ons to have a completely secure cloud solution.

Do small companies really need to worry about security?
Yes. Even if you don't keep much data about customers, in today's environment there are attacks on small businesses that can be devastating. For example W-2 theft is rampant, and can put all of your employees at risk of identity theft. Ransomware attacks are increasingly being targeted at small businesses, with hackers threatening to erase or lock businesses out of their data unless they pay a ransom.

How has my security vulnerability changed over the last year or two?
Malicious attacks are easier than ever to carry out, with malware kits available online to people who are looking for a quick way to steal information or perform ransomware attacks. Small businesses are facing a growing body of criminals who have found an easy way to threaten small businesses. While you may never experience the kinds of sophisticated, targeted attacks that financial institutions and large corporations face, today everyone is vulnerable because there are so many criminals out there, and the tools are freely available.

How often do I need to check my security protocols?
Quarterly security and IT checks are recommended.

Should I use an independent vendor to check my IT and security?
Yes. Whether you are using an in-house team or a managed IT vendor, it's best practice to have an independent audit performed annually.

Gary Thomas
Leap ManagedIT

Gary is a small business leadership guru and sought after cyber security speaker. He successfully led the transformation of a near century old organization into a leading-edge technology company where he currently serves as president. Along with serving on several non-profit boards he is also a world class competitor completing 8 Ironman triathlons.

Michael Thomas
Leap ManagedIT

Michael is a Fortune 200 veteran where he led a nationwide group that was dedicated to teaching organizations how to leverage technology, insights and data to drive innovation. He is also the co-founder of an early stage drug development that is focused on developing 'smart' therapies. He devotes his free time to serving on a local youth sports board along with coaching basketball, lacrosse, and soccer.

Security

3 MINUTES TO A STRONGER COMPANY

CEO Guide to Understanding IT

Security: Knowing IT's really protecting your business

Information security is like any aspect of your business backend: as the CEO, you don't need to know the details, but you do have the responsibility for oversight. After all, your computer systems are a critical business tool, and if anything goes wrong, it impacts your entire business.

In this 3-minute tech-check you'll get specific quick steps you can take regularly to check in on your company's security.

LEAP MANAGED IT

Gary Thomas and Michael Thomas

leapmanagedit.com

MINUTE 1

THREE QUICK QUESTIONS IN FIVE KEY AREAS

The most basic level of security means you have the following 5 items in place in your company:

- Antivirus
- Malware protection
- Firewall
- DNS protection
- Data encryption (including encryption of email and backups)

For each of these ask 3 questions to your IT manager:

- Do we have it?
- Is it enabled and fully configured for every computer/location in the organization?
- When was the last update of the software/hardware?

Your IT manager should be able to provide you with a scorecard compared to the best practices in the industry on a quarterly basis.

By the way, using a cloud service does not automatically mean your company has these items covered. Depending on the cloud service you use, security may be built in, or you may need to purchase and configure your own security services from the cloud provider or independently.

MINUTE 2

WHAT IS THE COMPANY POLICY? HOW IS IT ENFORCED?

Security isn't just what happens inside your company. Employees may be working from home or from a public WiFi spot. Files can be brought into your company from other sources, such as thumb drives, devices, and peer-to-peer networks. Employees may be using their private computers or devices to view company information.

Ask your IT department these 5 quick questions:

1. What is our company security policy regarding work outside of the office and devices other than company-purchased devices?
2. What is the procedure for closing all user accounts for employees who leave the company?
3. Where are the written copies of these policies?
4. How are you ensuring that employees know the security policy?
5. How are these policies enforced or monitored?

By the way, if you don't get past questions 1 and 2, you're not alone. Take the time to meet with your IT manager to create appropriate policies for your organization.

MINUTE 3

TRAINING

Untrained employees are often the most dangerous security risk to your company. Approximately 60% of security breaches are caused by employee mistakes that could be prevented if employees were properly trained.

To check whether your employees have the appropriate training, ask any employee the following questions:

- Have you ever gotten a suspicious email? Under what circumstances do you refrain from clicking on a link in an email?
- Do you use public WiFi locations for any company work? What kinds of activities do you do or refrain from doing when you are in a public place?
- What files in the company do you consider to be sensitive/secret? How do you make sure they don't get into the wrong hands?
- Do you use secure passwords? Have you ever given your password to someone or used someone else's password in the company? How often do you change passwords? Do you use the same password to log into multiple systems?

If remote work is important to your company, talk to your IT manager about secure transactions and using technology such as VPN and file encryption to ensure secure file transfer in and out of the corporate network.

BONUS MINUTE:

CONTRACTORS AND VENDORS

If you are working with remote employees, contractors, vendors or other organizations, it's important to know that they adhere to the same security standards you do. For example, your attorney and accountant have access to extremely sensitive documents from your company. If you are using off-site services such as these, make sure your IT manager is holding them accountable and have the proper security protocols in place.

Ask him or her to spend 3 minutes reviewing this tech check with anyone who has access to your company's proprietary materials.

leapmanagedit.com