YOU ARE NOT IMMUNE TO

I.T. WOES

DO NOT IGNORE

THE SYMPTOMS

IT may not be your thing. Running a small business requires you to juggle many responsibilities. It might seem easier to ignore that software alert or slow-running system, but turning a blind eye to IT issues could have disastrous consequences.

This ebook examines disregarded warning signs, the dangers involved, and what to do about symptoms of IT ills.

There are those of us who run to the doctor at the first sign that something might be wrong, whereas others fight through the symptoms and ignore the warning signs. They'll do something when it gets really bad, right? This can be a terrible idea with your health, and it's also a risky tactic to adopt when it comes to your business IT.

Problems with IT can become serious issues with major implications for your organization. Yet you overlook the current annoyance because you've got bigger things to worry about or a deadline to meet.

You've noticed the server isn't responding quite as fast as it used to, but a slow-to-respond server could mean a failing hard drive. Or it might indicate that your server has been hacked. The server can't do your jobs, because it is busy taking part in cyberattacks on other servers.

You may have employees see an error message and press the X to make that alert window go away. They might worry that raising a concern will draw attention to software they've installed on their own (not a good thing!), or they may not want to bother someone to ask for tech support. Maybe they figure it will make them look bad, take too long, or cost too much. So, they ignore the warning signs.

Meanwhile, that "minor issue" is festering and can end up disrupting the entire organization if left untreated.

The Risks of Ignoring IT Issues

Closing an alert notification every time you log in for the day is such a small thing to do, right? And you get to go about your day. Everything seems to be working fine anyway. But a little IT alert can turn into something big and dangerous, and some businesses never recover from a bad cybersecurity incident.

It seems like there is a fresh news story each day about a big business suffering a data breach. The small businesses hit by cyberattacks don’t make the headlines, but don’t let that fool you. Everyone, regardless of industry or business size, is at risk.

At the least, downtime due to a data breach or ransomware attack is going to cost you. There's business productivity lost and the expense of remediating.

In addition to the financial loss and resources expended, you could also face:

Damaged Reputation		A Damaged Reputation
	Compliance and Regulatory Fines	
Employee Attrition		Missed Business Opportunity

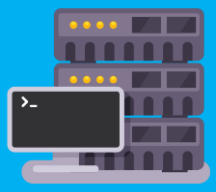
Cybersecurity needs to be a high priority. With IT running seamlessly, your business remains efficient and employees are productive. Your individuals can turn their attention to innovating and developing a business advantage.

Important Steps to Take

Avoid getting caught off guard by a major IT problem. Make sure all your employees are aware of the risks of taking a head-in-the-sand approach to IT concerns. Emphasize the importance of patching servers and workstations, and keep antivirus and firewalls up to date. Ignoring an update because it takes a few minutes to load could lead to hours, even days, of downtime.

Put a strict password policy in place, as well. Two-factor authentication is a good idea. A bad actor with stolen credentials also needs an individual's personal device to get access. It makes the crime more challenging, which can act as a deterrent.

It's also critical that your business knows what IT is has. This can include:

	**Understanding what is installed on the server and who has access.**
	**Making sure all installed software is licensed and supported by the manufacturer.**
	**Keeping an updated network schematic;**
	**Knowing the admin passwords for all your servers, routers, major applications, etc.**
	**Finally, install a reliable backup system.**

Yeah, yeah, you know this one already, but have you done it?

Many businesses have the intention of getting around to this but don't act to set up a backup solution that saves information both online and on various media.

Follow best practice and back up in three places. You might have one on a local, on-site computer, but you'd also have a backup on a remote device and another in the cloud. The cloud one offers flexible access anywhere. Also, actively test the backups to ensure they're doing what you want them to do. An issue with a backup is not something you want to discover in the midst of a data breach.

Insure Your IT Works Well, Securely

IT is the backbone of business, especially today. Think of IT expense as an investment in business success. Close attention to your IT also insures you're not taking unnecessary risks. Every business has sensitive files, whether a secret sauce or customer data.

Still, you started your business because you were great at something other than IT. Partner with a managed service provider (MSP) to sort out your cybersecurity. The MSP's experts can check server and workstation hardware and keep up with error messages. They can set up good backups (local and remote) to prevent catastrophic data loss. Plus, they can provide employees with an easy way to report IT issues to avoid the "I didn't want to get IT involved" risks.

Leave the IT to us so you can give your full attention on the other areas of your business success. Contact us today at 508-617-1310.

You Are Not Immune to IT Woes. Do Not Ignore the Symptoms

Phone: (508) 617-1310

Email: info@powerupboston.com

Web: www.powerupboston.com

Facebook: facebook.com/powerupboston