MYsherpa®

Business Technology Guides™

Get better results by avoiding these 7 critical mistakes.

A handy guidebook to worry-free IT.

mysherpa.com

Hi.

Most companies don't realize how much their IT systems are costing them.

Little inefficiencies turn into thousands of dollars in lost profits over time, and bigger problems like a server crash or a data breach can threaten to take a business under.

Yet despite the importance of technology, many companies settle for putting up with daily IT annoyances and cross their fingers that a catastrophic problem won't happen. Then, if a big issue does arise, they have to hope their IT provider will come through. Sometimes they do. Sometimes they don't.

At MySherpa, we've helped hundreds of businesses take a more proactive approach with their IT. In the process, we've found dozens of ways to save companies time and money.

We wrote this PDF to share a few of the biggest ones with you.

You deserve to be able to focus on your business and not worry about your technology. By taking action on even one of the items below, you'll save yourself a ton of headaches—and a ton of money, too.

Let's Chat!

Mistake

1

Inefficient New Hire Onboarding

Do you have a *seamless onboarding protocol*? If not, you are likely wasting a lot of money in the process.

A bad onboarding system can look like this: the day before a new hire starts, the manager realizes they forgot to set up her PC. A panic email goes out to cobble something together. An old computer gets pulled from the bottom of the storage closet, and as the team hurries, the new hire's last name gets misspelled in the new user profile.

This error doesn't get discovered until the following morning when the new hire can't log in. After waiting an hour for the mistake to get resolved, she finally gets access and can get to work. Then, after lunch the machine crashes. It turns out her computer should have been put in the decommission pile, but it got stuck in storage instead. She now has to work on an old machine that crashes three times a day while the new one is on order.

***Worry-free IT tip:* Don't let a story like that happen to you. Commit to a seamless IT onboarding process. It will make a great first impression and will decrease the cost to start new hires by up to 300%.**

Let's Chat!

Mistake

2

Doing IT on a Time & Materials Pricing Model

It sounds smart to pay your IT provider only when you need them. The problem is, though, *this approach tends to be short-sighted*.

While a company's systems are humming along, it can be easy for them to forget that software and security requirements are constantly changing. As the days go by without any problems, their systems become sluggish and behind the times. Then, when something does happen, it costs a ton of money to fix because of all the time and latent updates involved. Even worse, the company then has to pay salary during their employee's downtime—which could have been minimized or avoided with a more proactive IT approach.

Most businesses are so used to this "fix-it" type of IT model they don't realize there's a better way. By focusing on preventative maintenance and keeping systems at peak performance, companies keep their staff happy and at high levels of productivity.

***Worry-free IT tip:* While it seems like the "fix it" model saves money each month, flat-fee IT services are an investment in your business that yield big return.**

Mistake

3

Data that's not secure

A lot of companies think their data isn't a target for hackers. As a result, they get lax about data security and position themselves for a catastrophe.

Hackers rent hacking software that probes the internet for vulnerabilities. This process is automated and impartial, and it makes the hackers' jobs easy. When they gain access to a company's system, they can steal data or render the business's computers inoperable. At that point, fixing the problem becomes an expensive nightmare.

The hidden expense, though, is the cost of *employee downtime* while the situation gets resolved. To use a $10M company as an example: every day they're down will cost them about $40,000 in lost revenue. If it takes a week to restore the system, a simple ransomware attack costs them well over $200,000.

Worry-free IT tip:
Don't gamble with your data security. If you do, you're betting against your bottom line.

Let's Chat!

Mistake

4

Not having the right backup system

Backing up your data on the cheap costs you tens of thousands of dollars over time.

Many of the business owners we talk to say, “My IT people tell me my data is backed up and off-site. I’m good, right?” Maybe, but usually not. To make sure they have the right system for them, businesses need to consider two things—their system’s *Recovery Point* and *Recovery Time Objective*.

Recovery Point is the technical term that means how often the backups are running, and by implication, how much work might get lost if the system crashes. For example, if you back up once daily, then a business will always risk losing up to a day’s worth of work. For the hypothetical $10M company, losing a day’s worth of work could equate to $40k. This figure can then get multiplied several times over if a system’s *Recovery Time Objective*—the amount of time it takes to restore the data—is slow.

***Worry-free IT tip:* It’s worth it to make sure you have the right backup system. When compared against the cost of downtime, we find that only about 2 out of 10 companies do.**

Let’s Chat!

Mistake

5

Having employees that go phishing

When it comes to hacking, your biggest vulnerability isn't your system—*it's your people*.

If a hacker can get an employee to click on a malicious link or trick them into sharing confidential information, that's all they need to wreak havoc on an IT system and tank your profits and productivity.

Many companies combat these phishing tactics by doing an occasional staff training. That's a great first step, but it often falls short because classroom-type learning can only go so far. *Simulated phishing programs* are the next step up. With simulated phishing, staff get sent randomly timed emails that mimic the hackers' tricks. This approach keeps employees on their toes and up-to-speed on what to look for. Also, it keeps the company safer from any click-happy staff. By doing simulated phishing, mistakes become learning opportunities, not giant problems.

***Worry-free IT tip:* Invest in a simulated phishing program. Doing so will greatly improve your overall security by reducing the risk of an employee-caused breach.**

Let's Chat!

Mistake

6

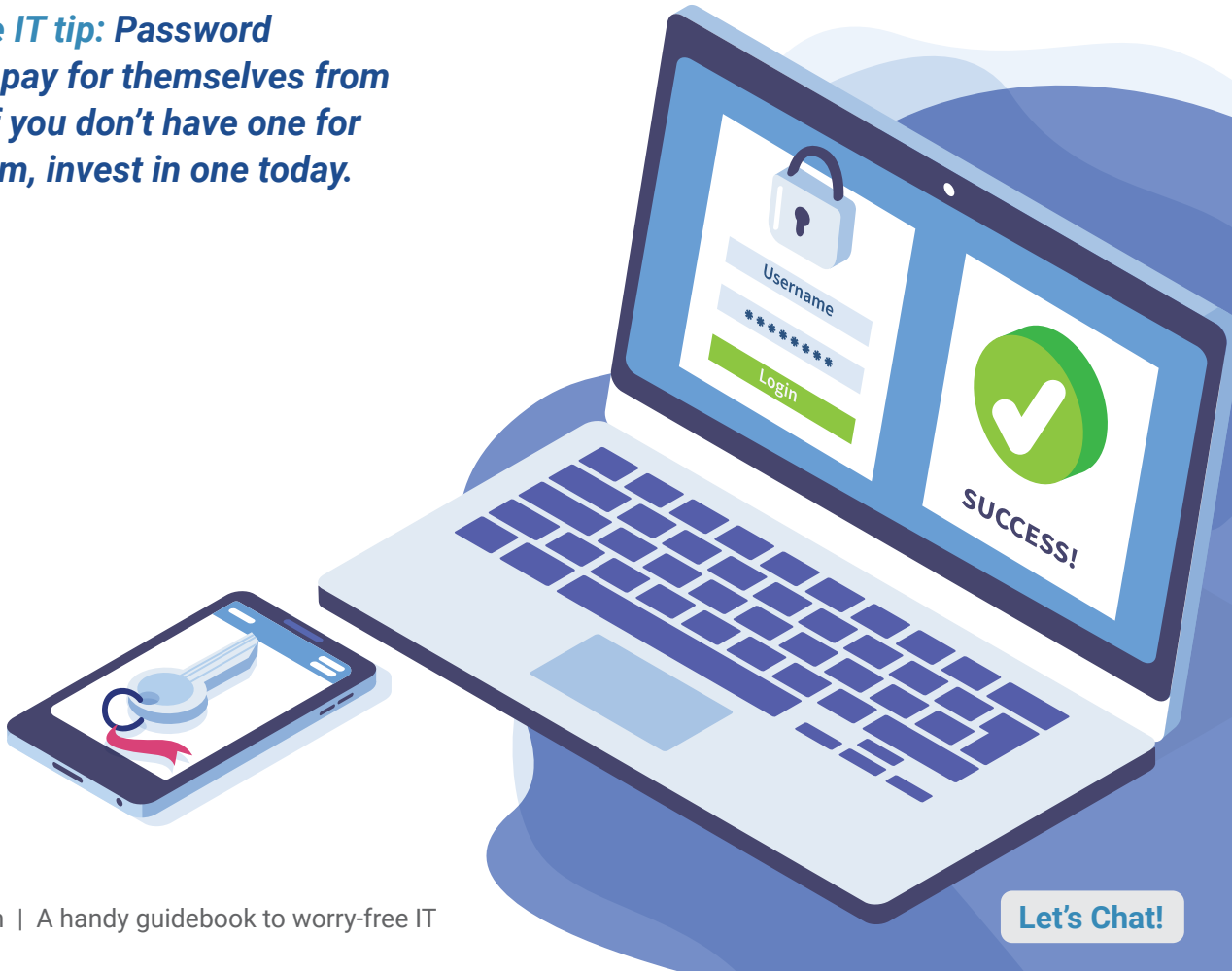
Everyone has their own passwords for everything

Having to remember a lot of passwords is a pain—one that hurts a business's bottom line.

Forgotten passwords don't seem like a big deal until you add up all the time that employees spend trying to remember them. Together, those brief moments turn into thousands of dollars of wasted salary each year.

Central password managers are an inexpensive way to keep employees from playing the password game. They only need to remember one central password, and the password manager takes care of the rest.

***Worry-free IT tip:* Password managers pay for themselves from day one. If you don't have one for your system, invest in one today.**



Let's Chat!

Mistake

7

A Lack of Computer Standardization

When a business doesn't standardize their computers, the costs add up quickly. At first, though, it can seem like they're actually saving money.

Let's say employee Susie Q's laptop dies, and it gets replaced by a "Best Buy Special." It was on a screaming sale and has some new bells and whistles, so at first it seems like a win. But no one realized it had Windows Home, not Pro. To get it compatible with the network, the department has to pay for an upgrade. Also, they've already paid half a day's salary to acquire and set up the machine. Then, Susie starts working on it and discovers it's slower than the old computer. Her loss in productivity over time turns a "good deal" into a horrible one.

By setting *computer standards*, a company takes all the variables out of getting a new machine. They can quickly replace a computer with an equivalent or better model, and they can even keep a spare or two on hand so no one has to wait if their machine goes down.

***Worry-free IT tip:* Increase staff efficiency and decrease stress by setting computer standards and proactively updating them.**

Let's Chat!

Let's chat.

Little IT issues increase stress and can add up over time.
But they don't have to.

If you want help making your IT worry-free, we'd love to talk.

Schedule a call with us today, and we'll chart a course to improve your IT—and along with it, your productivity and bottom line.

Schedule My Call

MYsherpa®

Business Technology Guides™