TOP 10 MISTAKES BUSINESS OWNERS MAKE WITH IT

I've seen time and time again the same mistakes being made with how businesses treat their often-expensive IT investments. It wasn't the fault of the technology itself. It was decisions that were being made that led to companies NOT getting the bang for their IT buck that they should be.

This chapter is a lengthy list of IT mistakes I have seen made by business owners, executives, managers, etc.

First, Let's Talk About Money!

Mistakes and shortsightedness in IT can and will cost the business owner money, and sometimes, lots of it. Here are the mistakes I have seen made:

1. **Treating your IT like an expense and not an asset!** Too often I meet business owners that roll their eyes and sigh when it comes to investing money in IT. I hear, "It's just too expensive," or "Why do we even need that?" or last but not least, "I hate IT." Yet these same businesses would be in a world of hurt if something happened to those computers! Good IT makes money for the business by improving staff efficiency. Think about it—payroll, accounting, customer tracking, invoicing, and purchasing are all done on a computer to save time, which equates to quicker response and fewer staff on the payroll. Yet the care and feeding of these critical computer systems is often neglected and underfunded. It's an asset that saves money, so invest wisely in it. Don't get the el-cheapo computers from Best Buy or Staples. Buy quality so they last longer, have few problems, along with better performance. Your IT Pro can help with that!

2. **Putting up with slow, buggy computers and networks.** I've seen staff members hampered by slow internet, aging computers that lock up, and printers that won't print. (OK, all printers ARE evil!) Every minute the staff spends waiting on a page to load or clearing the paper jam or rebooting a computer is money lost to the business owner. One office manager in particular I worked with hated all things IT because he didn't understand IT. He also wanted the bottom line on the books to look good for the owner, so he kept the workstations around for seven, eight, ten years, well beyond their usefulness. The staff knew better than to complain to him about slow computers, but they didn't hesitate to tell me or my staff their frustrations. I brought it up to the office manager, and the promise of new computers was always pushed off to the next quarter or the next year. I ended up firing that client because the office manager held me accountable for the performance of these geriatric workstations. Give your employees quality tools and watch the productivity increase, not to mention job satisfaction. If your bookkeeper is running the payroll on an eight-year-old computer, trust me, you are losing money and are taking a risk of missing paychecks and alienating your most important asset—your employees.

Second, Let's Talk IT People

The advancement of technology in the late 90's saw an increased demand for IT talent. Being a nerd became cool. (Thank you to *The Big Bang Theory*!) Here are the mistakes I have seen companies make with hiring IT people:

3. **Thinking that one IT person can handle it all.** Back in the 90's, I did it all—hardware and software expert, database designer, printer repair, cable installer, network engineer, and phone expert. The world of technology has grown exponentially in the past two decades. In fact, technology is the fastest changing industry. It has evolved into so many areas of specialization that one person cannot absorb it all. I would be lost without my team. Having experts in different areas of IT provides the best solutions. Don't let your IT person be an island! Hiring an outside IT provider that will team up with your internal IT can help streamline your company functions and give your IT person the benefit of experts in different areas of IT. I will talk more about this co-managed arrangement in Section Three of this book.

4. **Believing hiring good IT is easy.** Right now, there is an incredible demand for IT people ever since COVID-19 hit. Work-from-home allowed companies on the West Coast to offer big money to cheaper at-home talent in other states where the cost of living is much less (i.e., Kentucky!). It's really tough for anyone, including myself, to compete with those corporations with deep pockets. We got several clients because they just gave up on hiring in-house when they had such difficulty finding a quality person that fit their budget. Sometimes the clients offered more money but didn't know what questions to ask to verify they had a qualified IT person. I have learned that a lot of people go to school for IT because they believe they will make a lot of money, but at the same time, a lot of them don't have the right mindset for IT. The college machines are turning out a lot of IT people who are good at taking exams but poor at problem solving. One field that I see as oversaturated right now is degrees in "cybersecurity." Graduates have images of six-digit salaries in their heads and find that there are no jobs but the most basic ones because they have zero experience in the field. They often don't know the basics of how a packet of data gets from point A to point B on a computer network. We always get a bunch of applications from these newly minted "security experts," and rarely do they qualify for my most basic tech job.

5. **Hiring a person with a "knack" for computers to save money.** IT is complicated, right? So, why would you hire someone who has a "knack" for it but no real-world experience or who has been given the responsibility on top of their regular job? I see this a lot to save costs on hiring a dedicated IT person or a way to avoid outsourcing IT. It works until it doesn't, like when the IT issues pile up, efficiency drops off, and Suzy in accounting clicks a link and you don't know what's going to happen next. You are better off outsourcing IT support to a qualified Managed Service Provider (like me!) and letting your employee with a "knack" for IT do something else. A quality IT person will solve problems faster and build defenses into your network in case an employee clicks the wrong thing in an email. We have a client who hired us to help their full-time employee that had a "knack" for IT. Their former IT consultant retired, so this employee took over the IT for about a year before we were hired to help. We found a massive

computer network rife with slowdowns and serious server issues. The aging Exchange email server was crawling along, and there were no backups. It took me and my team about a year to get the aging equipment replaced and existing IT issues fixed.

6. **Not inviting IT to the management meetings.** It's tough when the IT department is the last to know about company decisions that impact the IT infrastructure. Involve your IT in executive meetings. It's no fun when a major decision is made to remodel the building and the $50,000 needed to upgrade IT infrastructure was not included in the budget. If your IT is in-house or hired out to a company like mine, then include us. I remember one of my clients planned to build a beautiful new veterinary clinic complete with surgery rooms, grooming area, kennels, and a spacious waiting room. However, there was little thought given to where their file server was going. Luckily, I got hold of a blueprint and was able to coordinate a seven-foot-tall rack with shelves and *patch panels* to hold their server, switches, *UPS*, monitor, and keyboard. I was unable to get a dedicated thermostat for the IT closet, so the door had to stay open to keep it cooled properly. I didn't win the cooling battle, but at least they have a nice space that just fits their IT needs. This was hardly the first time I had seen insufficient planning for IT in a new facility!

Third, Managing Cyber Security

Cyber security is all about establishing a good defense. Let's look at these mistakes I see made about cyber security:

7. **Thinking that multifactor authentication is too much of a hassle.** There's an inverse relationship between strong cyber security and convenience. I had a new client come to me saying cyber security was their priority because they couldn't afford to take risks with their biggest customer's data. One of the first suggestions I made was enabling *multifactor authentication* (MFA) on their email logins. Well, she would not implement this because it would be too much of a hassle for her staff to spend a few minutes a month typing in the code. Yes, it's a hassle; my staff must deal with it too. But with email being the number one entry point for hackers, it becomes a question of a little inconvenience versus losing your biggest customer. So, if you are too focused on convenience, then chances are your cyber security is lacking in key areas. Now there is a balance that must be struck between security and convenience as long as you understand the risks. Multifactor on every single login to email from a secure company computer isn't necessary if other safeguards are in place. I know it would drive me crazy to face entering multifactor codes all day long.

8. **Thinking cyber insurance isn't necessary.** A cyber insurance policy is a must for business owners who rely on computers. Your computers are just as critical as your company cars, employees, and office building. Don't guess what you need; talk to an insurance agent that specializes in cyber policies so that you know what is and what isn't covered. Be sure to ask who pays if your company email is hijacked and used to steal money from other companies. You will read a story in Section Two on how one of my clients had a really close call with their email being hijacked, and if it had been successful, their cyber insurance would not have covered it.

9. **Thinking your company is too small to be hacked.** Does your company handle money? If yes, then you are a target. In the last section of this book, I will tell a story about a very small company that got swindled out of $380,000. Targeting a small business really paid off for those scammers! All US-based companies are a target and are worth the time and trouble. They also know that small businesses have fewer resources to dedicate to cyber defenses, so they make wonderful targets for hacking.

And Lastly…

10. **Wanting someone to write a custom application for your company.** From time to time, clients ask me about writing custom business applications. I took programming classes for my bachelor's degree and did some database programming for a federal contractor after I graduated. Writing FoxPro database programs gave me enough insight into the difficulty of writing and maintaining code. There were never-ending requests for new reports and updates to how the databases were organized. Back then, the operating systems weren't changing as quickly as they are today, and the cyber security risks were minimal. Custom applications nowadays will need care and feeding by the developers their whole life. New versions of Windows/Mac and new cyber threats means regular updates to the code, not to mention features and reports you want added over time. Also, it's extremely difficult and expensive to find someone to work with your code if your original development team abandons it or you for whatever reason. I do encourage clients to bend a little on the existing market offerings and talk to others in their industry to get recommendations.