What's New

4 Mistakes People Make By Being Cheap With Technology

Technology today is more affordable and accessible than it's ever been and it's increasingly important to consider the balance between cost and quality. There are many small businesses that continue to cheap out on their technology and IT solutions. They don't want to commit to quality hardware, software, security or backups, etc. and instead they go for the cheapest solutions, which often means they spend nothing at all. They don't commit to reliable security or current software and they set themselves up for disaster.

The question is, are you setting your own business up for disaster? Here are four critical mistakes to avoid:

#1: *Not Backing Up Data.* As convenient as it is to have all of your business's information in one place, like on a single local server or PC, you're toast if anything happens to

that hardware. If you're lacking in IT security, you're making a cybercriminal's job easier and when that hardware fails (as hardware eventually does), you're left scrambling to recover your data and hoping it's still accessible.

You should never risk your business like this—especially considering how easy it is to back up your business's data. You can back up data on-site, get a cloud-based service or both. You need to back up everything so you're ready should anything go wrong.

Once you have a solution, you can customize how your data is backed up. Do you need to back up data every day? Week? Month? It's up to you! Another thing to remember: your backup system isn't "set it and forget it". Be sure to check on it regularly and keep it updated to ensure your data is safe and ready to go should you need

it.

#2: *Not Keeping Up With the Times*. You should always update your software. Developers are constantly fixing bugs, patching software and improving usability. Skipping updates can leave you vulnerable.

Earlier this year, Cisco's Series 1001-X router was found to have a fatal flaw that opened it up to hackers. This flaw potentially gave hackers network access – and access to connected devices. Cisco pushed out an update to fix the flaw, but the update is useless if you don't install it.

Updates also apply to hardware. When you're running old hardware, that hardware is more likely to fail. It's already been put through its paces. Over time, hardware performance degrades. Plus, the older your hardware is, the less compatible it is with current software. You don't have to invest in new hardware every year or two, but keeping up with the times keeps you on top of your game.

#3: *Not Training Your Team*. While most businesses hire people who understand certain software products, you can't assume they know everything about that software. Your business might use a certain CRM application in a very specific way. Proper training on your systems ensures everyone is on the same page – and that they are using the software to its (and their) greatest potential.

In addition, your team also needs to be trained on IT security. They need to know the risks and how to keep your business's data secure. Never assume your team knows about the latest threats to small business – or that they even understand the basics of safe web browsing.

While you need to have IT security in place and

protecting your network, servers, PCs, etc., you need to make sure your team understands that security and the threats that are out there. Your team should also be aware of the consequences if any data becomes compromised.

#4: *Skipping Data Security*. Data breaches happen every day, and most of them go unreported. You only hear about the biggest breaches on TV or online. While major companies like Facebook can more easily recover from a data breach, most small businesses can't.

If you're lacking in IT security, you're putting sensitive data at risk. This is proprietary business data as well as the personal and financial records of your customers. It can mean the end of your business if credit card numbers, names, addresses or phone numbers fall into the wrong hands.

Customers will no longer trust you. Your own employees likely won't trust you either, especially if their personal data is on the line, not to mention their reputation. When you skimp on IT security, you're about one step away from handing hackers and cybercriminals all the data you should be keeping under digital lock and key. When you invest in a solid IT security and work with experts who understand today's security landscape, these are things you don't have to worry about.

The bottom line is, if you don't invest in your business's technology and IT solutions today, you will pay for it tomorrow. You'll be dealing with upset customers if you get hacked, and you may end up closing your doors, temporarily or perhaps even permanently, as you attempt to recover lost data. Don't make these mistakes because you wanted to save a few dollars.

Tips for Protecting Remote Employees From Cyberthreats

Don't Use Unsecured Public WiFi

Unsecured public WiFi is everywhere: at cafés, airports, hotels and more. But these networks lack security, and it's easy for a hacker to snoop on your data. Hackers can even spoof unsecured WiFi networks and walk away with all the data they want with no one the wiser. Avoid them. Have your remote workers stick with secure networks you can verify as trustworthy.

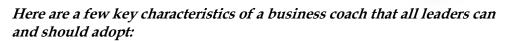### Don't Keep Your Cyber Security "Best Practices" To Yourself

You may have your best practices, but do your remote employees know? Keep EVERYONE on your team educated and on the same page. When you have training, bring in your remote employees, or conference them in, so they get the same training. Also be sure to send out regular updates about the latest cyber security threats and scams.

Don't Forget About Endpoint Security

Make sure your remote employees are utilizing IT security solutions on their end, such as antivirus software, malware scanners, network firewalls and even a VPN for when they need to access unfamiliar networks. They should also be keeping their software updated with the latest available patches.

Inc.com, 2/12/2019

Leading Like A Business Coach

Here are a few key characteristics of a business coach that all leaders can and should adopt:

LISTENING
Hearing is the physical act of sound going into your ears, but listening is about comprehension. The only way I can help groups improve is by knowing what works well and what their pain points are. They may not always say things you want to hear, but it's important that you truly listen. Don't immediately start problem-solving your way out of the conversation or you'll miss what's truly important.

LOOKING FOR WEAKNESSES
As leaders, we sometimes want to ignore weaknesses and problems because, frankly, it can be tough to admit they exist. You may hold some or all responsibility for them. But that's how a leader can push his or her company forward – by taking a high-level view and objectively finding the areas that need to be improved.

FINDING SOLUTIONS
After pinpointing shortcomings, figure out how to repair and strengthen them. It's not enough to acknowledge them; you also need to find solutions. Push your company or leadership team to sit down and brainstorm together. It's the best way to get everyone talking and to get others' perspectives on what will best address each issue. These sessions should be a regular part of the business's proceedings, not just when I'm there coaching.

LEARNING CONTINUOUSLY
It's helpful to know what leaders are doing in other companies. Read books and articles to see how others have improved their companies. Their solutions may work for you too, or they may spawn a brand-new idea you can implement. Even business coaches don't have all the answers, so take advantage of the world of resources at your fingertips to find a way around any roadblocks.

Leaders should never stop pushing and growing. That mentality will transfer to your team – after all, they are the ones who help keep your business going. Think, "What would Andy do?" and apply these principles in all meetings and company get-togethers, not just quarterly planning meetings. That's how the student can become the master.`

The founder of Petra Coach, Andy Bailey shows organizations the logjams thwarting their success, and coaches them past the excuses we all use to avoid doing what needs to be done. Andy learned how to build great organizations by building a great business, which he started in college. It then grew into an Inc. 500 multimillion-dollar national company that he successfully sold and exited.