the NetWork

LeadingIT

Chicagoland CybersecurITy Support

November 2024

How to Choose the Best Hardware for Your Growing Business

How to D.E.F.E.N.D Your Small Business Against Ransomware Attacks

Was Your Information Compromised From The National Public Data Breach?

5 Signs Your Business Might Need Managed IT Services

LeadingIT Core Values Victor of the Month

GoLeadingIT.com 815-788-6041 @goleadingit

How to Choose the Best Hardware for Your Growing Business

Growing a business is an exciting journey, but it comes with its own set of challenges, especially when it comes to technology. As you expand, ensuring you have the right hardware can make a world of difference in how smoothly everything runs. But let's be real: choosing the right equipment can feel overwhelming. That's why tapping into the expertise of your Managed Service Provider (MSP) is important. They can guide you to the best hardware options that fit your needs and help you avoid those costly mistakes that can come from buying tech that just doesn't cut it.

Step 1: Know Your Needs

Picking out new tech can be fun, but before you add anything to your cart, take a moment to figure out what your business needs. Ask yourself:

- What daily tasks will this hardware do?
- How many users will be relying on this hardware?
- What essential software do we need to keep things running smoothly?
- What's our budget looking like?
- Will we need portable options for remote work?

Did you know that around 82% of small businesses fail due to cash flow problems? Investing in hardware that doesn't meet your needs can definitely contribute to those issues, which is why understanding your needs is critical to help steer your IT purchases in the right direction.

Step 2: Lean on Your MSP for Support

Think of this as step 1.5: Don't be afraid to reach out to your MSP as you evaluate your needs. Your MSP isn't just there for emergencies; they know the ins and outs of what will work best for you. Armed with knowledge about your operations and answers to the questions we just covered, your MSP can offer valuable insights and tailored recommendations. Plus, they can help you make the most of your budget, ensuring your technology supports rather than hinders your growth.

Step 3: Consider Your Software Requirements

Not all software is created equal, and each type has its own hardware needs. Whether you're working with design software that eats up resources or simpler tools for day-to-day tasks, your MSP can point you in the right direction.

Fun fact: Businesses waste about 30% of their IT budgets on unnecessary tech. Your MSP can help you steer clear of that waste.

Continue reading on page 7

Pictured on the cover: Daniel, Jeremiah, Kelly

Was Your Information Compromised From The National Public Data Breach?

National Public Data confirmed in September 2024 that a hacker has compromised the personal records of millions of individuals. The information exposed includes the names, e-mail addresses, mailing addresses, phone numbers and even Social Security numbers of up to 2.9 billion people. Here's what you need to know.

What happened?

National Public Data, a consumer data broker that specializes in providing criminal records, background checks and other forms of data to private investigators, consumer public record sites, human resources, staffing agencies, the government and more, was hacked. The incident is believed to have started in December 2023 when a third-party bad actor attempted to gain access.

In April, a cybercriminal named "USDoD" posted the stolen data online in a popular criminal community. On August 6, the stolen dataset resurfaced, this time posted for free to several breach forums for anyone to access and download.

The sensitive, personally identifiable information released included names, addresses, phone numbers, e-mail addresses and Social Security numbers for millions of people, some of whom are deceased. The data also contained previous addresses and, in some instances, alternate names.

The official data breach notice that was filed in Maine indicated that 1.3 million records may have been breached; however, some lawsuits are suggesting as many as 2.9 billion records have been exposed.

As the investigation continues, many cyber experts are finding that some of the data released was inaccurate, and aside from the Social Security numbers, most of it is already public and easy to find online.

So why is this breach dangerous if the information can be found with a quick Google search?

There are several reasons to be concerned. Having all this critical information in one place makes it easy for criminals to use the information needed to apply for credit cards and loans or open new bank accounts.

The information included, such as childhood street names or the last four digits of your Social Security number, are often answers to security questions and can help hackers bypass authentication and access your private accounts.

Some cyber experts are suggesting watching for a surge in phishing and smishing (phishing over SMS) attacks as well.

Can you be affected even if you've never heard of National Public Data or purchased data from them?

Yes! Just because you haven't interacted with them doesn't mean other organizations, businesses, landlords, etc., haven't leveraged their resources to dig up information on you.

Continue reading on page 6

How to D.E.F.E.N.D. Your Small Business Against Ransomware Attacks

Ransomware is a type of malware that encrypts your data, holding it hostage until a ransom is paid - hence the term ransomware. These attacks continue to be a significant threat to businesses of all sizes, but they're particularly detrimental to small businesses.

85% of organizations experienced at least one cyberattack in the 12 months prior. Of those affected, 80% paid a ransom, but just 75% recouped their lost data. Had these businesses implemented a robust ransomware response plan, they could have minimized the damage, avoided paying the ransom, and quickly restored operations.

Why Ransomware Response Plans Are Critical

Without a solid ransomware response plan, small businesses face financial loss, reputational damage, and operational disruptions. A well-structured plan can minimize these risks, ensuring your business reacts swiftly and effectively to a cyberattack. With threats constantly evolving, it's important to have a strategy that addresses both prevention and mitigation.

To create a comprehensive ransomware response plan, we use the acronym D.E.F.E.N.D.

D. *Detection*

Being able to take swift action is the first step in mitigating damage. Start by installing cybersecurity solutions that monitor for suspicious activities. Managed IT services can assist in setting up real-time monitoring tools to ensure threats are identified as soon as they occur.

Early detection gives your team the time to react before the attack infiltrates your entire network.

E. *Eradication*

Once the ransomware has been identified, the next step is to eliminate the threat. This involves disconnecting infected devices from the network to prevent further contamination. Think of it like containing a fire–by isolating the infected devices, you're preventing the "flames" from spreading to the rest of your network.

Alternatively, if you cannot isolate infected devices from the network, you should immediately power them down.

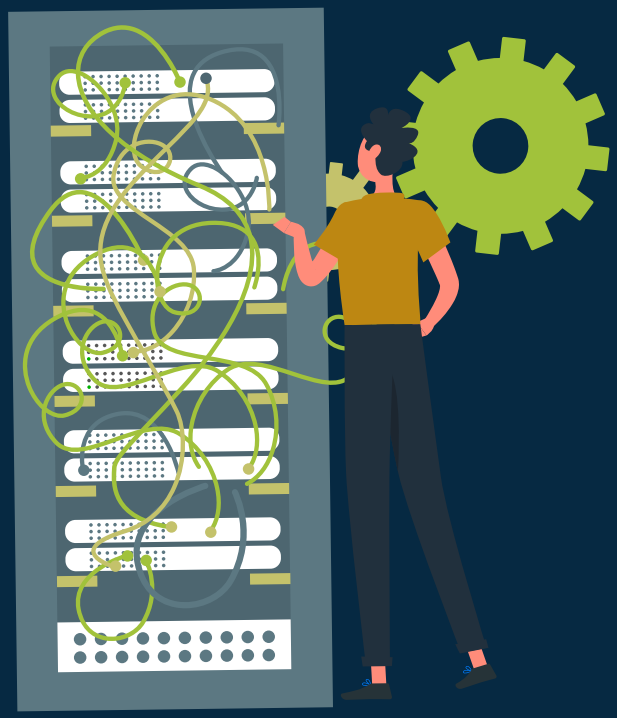
F. *Forensics and Reporting*

Documenting every aspect of the attack is vital for both internal analysis and legal reasons. Reporting the attack to cybersecurity companies and law enforcement is crucial for wider security efforts.

Small businesses can also work with their managed IT service provider to conduct a thorough investigation to understand how the breach occurred and what systems were impacted.

Continue reading on page 7

5 Signs Your Business Might Need Managed IT Services



Running a business is tough enough without constantly battling IT issues. If you're starting to feel like tech troubles are eating up too much of your time and sanity, it might be a sign that you need some outside help. That's where managed IT services come in, offering a way to save time, cut costs, and avoid endless headaches. Here are five clear signs that it's time to call in the experts:

1. You're Dealing with Frequent Downtime or IT Glitches

Nothing brings the workday to a screeching halt faster than technical problems. If your team is constantly losing time to system crashes or spotty network connections, it's more than just annoying—it's costing you money.

In fact, downtime for small businesses with fewer than 25 employees and just one server could run you around $1,670 per minute, or nearly $100,000 an hour. Think about that the next time your email server goes down for 30 minutes. Managed IT services can help by proactively monitoring your systems and fixing problems before they even have a chance to slow you down.

2. Your In-House IT Team Is Overwhelmed (or Non-Existent)

If you don't have an in-house IT team, you might be relying on the most tech-savvy person in the office to fix things. And even if you do have an IT department, they're probably stretched thin trying to manage everything from cybersecurity to software updates. Outsourcing to a managed IT provider gives you access to a whole team of experts without needing to hire, train, and keep specialized staff in-house.

3. You've Had a Security Breach (or You're Worried You Might)

Small and medium-sized businesses are a huge target for cybercriminals, and the cost of a breach can be devastating—not just in dollars, but also in terms of lost trust and reputation. Did you know that for businesses with fewer than 500 employees, the average cost of a data breach in 2023 was a staggering $3.31 million?

If that stat makes your stomach drop, it might be time to call in a managed IT service. These pros specialize in securing your data and staying ahead of the latest cyber threats, offering everything from advanced firewalls to data encryption and compliance support.

Continue reading on page 6

National Public Data Breach continued from pg 3...

What should you do to protect yourself?

STEP 1: Check to see if your data has been exposed. You can use tools like https://npd.pentester.com/ to find out if your information has been compromised. If so, it's important to take immediate action.

STEP 2: Request a copy of your credit report and then freeze your credit. One of the best ways to protect your identity is to freeze your credit and set up alerts. This prevents criminals from opening up new lines of credit in your name. To do this, contact all three major credit bureaus – Equifax, TransUnion and Experian – and request a freeze.

The process is free and should take you less than 10 minutes per site to complete. If there are others in your house over the age of 18, it's a good idea to freeze their credit too. Anyone with a Social Security number is vulnerable following a breach of this size.

Once you have a copy of your free credit report, review it for anything that you didn't authorize. Don't forget to set up alerts and review your credit regularly.

STEP 3: Watch out for phishing scams. As mentioned, many cybercriminals will try to leverage this information to scam you through phone calls, text messages, e-mails and even social media sites. Be cautious!

5 Signs Your Business Might Need Managed IT Services continued from pg 5...

4. Your IT Costs Are All Over the Place

Do you feel like every month, you're hit with some unexpected IT expense? Maybe a piece of hardware failed, or you had to buy new licenses for software. These costs can add up fast, and they're tough to predict. Most providers offer fixed monthly pricing, so you know exactly what you're paying for and can budget accordingly. Plus, they'll optimize your infrastructure, so you're not wasting money on unnecessary tech.

5. IT is Distracting You from Growing Your Business

This might be the biggest sign of all. If your day-to-day is filled with managing IT issues instead of focusing on what you do best, it's time for a change. Managed IT services let you offload routine tasks like software updates, backups, and troubleshooting, so you can spend more time on strategic initiatives.

The Takeaway

Your IT setup needs to work seamlessly in the background rather than be a constant source of stress. If you're nodding your head to any of these points—frequent downtime, security concerns, unpredictable costs, or a stretched IT team—it might be time to consider managed IT services. Outsourcing to IT experts can help prevent issues before they arise and free you up to focus on the important parts of your business.

D.E.F.E.N.D. Against Ransomware Attacks continued from pg 4...

E. *Endure with Proactive Measures*

Prevention is always better than the cure. To reduce the likelihood of ransomware attacks, it's critical to have proactive measures in place such as:

- Regularly updating your software and security protocols,
- Hosting employee awareness workshops, and
- Ensuring data is backed up regularly

In addition, many cybersecurity solutions offer tools like encryption and firewall protections, which act as the foundation for your defense strategy.

N. *Notification and Communication*

Once an attack is detected, immediately notify:

- Relevant stakeholders
- Employees
- Business partners, and
- Customers

Full transparency is key. It helps maintain your company's reputation and gives everyone the chance to take necessary precautions.

D. *Data Recovery and Containment*

Ensure your business has reliable backups in place so data can be restored without paying a ransom. Managed IT services can assist in restoring encrypted data from backups and help contain the spread of ransomware by blocking compromised entry points. Swift containment and recovery will allow your business to return to normal operations with minimal downtime.

By following the D.E.F.E.N.D. strategy, you're protecting your company from costly attacks and ensuring prompt recovery efforts if you do become infected.

How to Choose the Best Hardware for Your Growing Business

continued from pg 2...

Step 4: Assess Compatibility with Existing Systems

Before making any purchases, check how the new hardware will integrate with your current systems. Is your existing software compatible with the new hardware? Are there any connectivity issues you need to consider?

This is another area where your MSP shines; they can help ensure that new devices won't cause headaches down the line. Remember, a smooth integration can enhance productivity, while poor compatibility can lead to frustration and wasted money.

Step 5: Future-Proof Your Investment

You don't want to invest in something that'll be outdated in a few months. Talk to your MSP about future-proofing your hardware. They'll guide you toward scalable options that can grow with your business. Investing in solid equipment now can save you from those costly upgrades later.

The Bottom Line

Picking the right hardware for your growing business can be a chore. But with the right MSP by your side, you can make confident choices that fit your goals. Their expertise can give your productivity a real boost and let you focus on growing your business. So, make a point to check in with your MSP at every stage of the process.

LeadingIT Core Values Victor of the Month

This month, we are delighted to recognize James, our Level 3 technician, as the Values Victor for exemplifying Accountability. James consistently demonstrates an unwavering commitment to both our clients and our company. Not only does James take ownership of his tasks, but he also steps up to own any mistakes and ensures they are rectified promptly and efficiently. His dedication to holding himself and others accountable reinforces a culture of integrity and reliability at LeadingIT. Congratulations, James, on your well-deserved recognition!

LEADINGIT VALUES:

- We Are Driven
- We Chase Excellence
- We Are Humbly Confident
- We Are Accountable
- We Have A Positive/Fun Mindset

Continue reading on our blog at goleadingit.com/blog

LeadingIT

Serving the Chicagoland area with offices in Woodstock, Downtown Chicago, and now in Manteno, IL.

LeadingIT

$1000 REFERRAL PROGRAM

WE LOVE REFERRALS!

Do you know an organization that needs fast + friendly IT and cybersecurity support?

If they sign up, you'll receive $1000!

LEARN MORE

GOLEADINGIT.COM/REFER

815-788-6041

WE ARE CELEBRATING!

Birthdays

Giancarlo Jabon
November 8th

Anniversaries

Laura Piekos
11/26/2018