LeadingIT

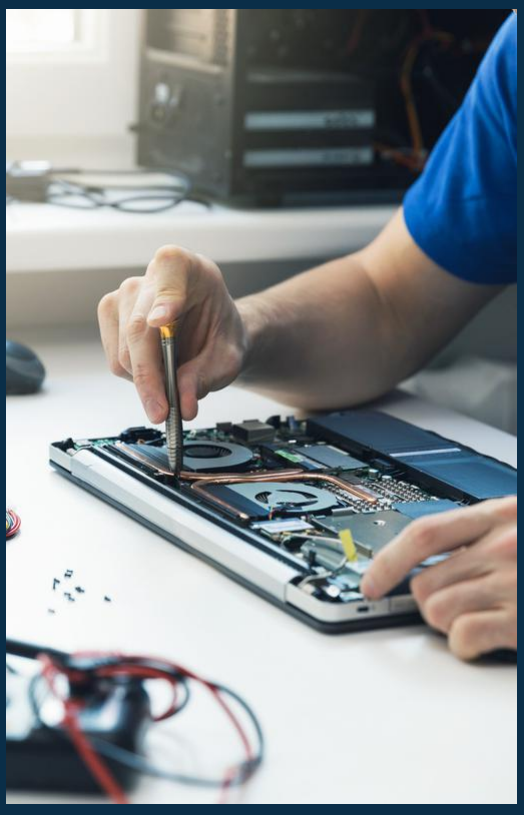
June 2025

The NetWork

- HOW LONG SHOULD BUSINESS LAPTOPS REALLY LAST? (HINT: IT'S NOT WHAT YOU THINK)
- WHY WE ENFORCE CYBERSECURITY TRAINING: PROTECTING PEOPLE, DATA, AND BUSINESS CONTINUITY
- WHAT'S A PATCH, AND WHY DO WE KEEP INSTALLING THEM?
- CYBERSECURITY ON A BUDGET: WHAT YOU CAN'T AFFORD NOT TO DO

How Long Should Business Laptops Really Last?
(Hint: It's Not What You Think)

If your business laptops are starting to feel sluggish, freeze up randomly, or take forever to load basic apps, you might be wondering: How long are these things supposed to last? It's a fair question—and one that's often misunderstood. Many business owners assume a laptop should last five to eight years. But the real answer depends on how you use them, how often you upgrade software, and whether your business is growing.



Let's clear up the confusion:

The Average Lifespan: 3 to 5 Years (With a Catch)
Most business-grade laptops begin to slow down or show signs of wear within 3 to 5 years. Even if the machine technically still works, it may not be doing your team (or your security) any favors.

Here's why:

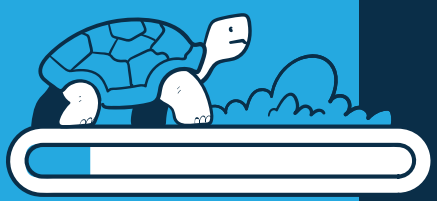
- Security Risks: Older laptops may not support the latest security patches or OS updates.
- Performance Drops: Newer apps require more power. Old machines struggle to keep up.
- Productivity Loss: Waiting 10 extra seconds every time you open a file adds up fast.

Still clinging to that 7-year-old laptop? It might be costing you more than you think.

Signs It's Time to Replace

Ask yourself:

- Does it take longer than 30 seconds to boot up?
- Are your employees complaining about speed or crashes?
- Is the laptop no longer compatible with updated software?
- Are repair costs stacking up?



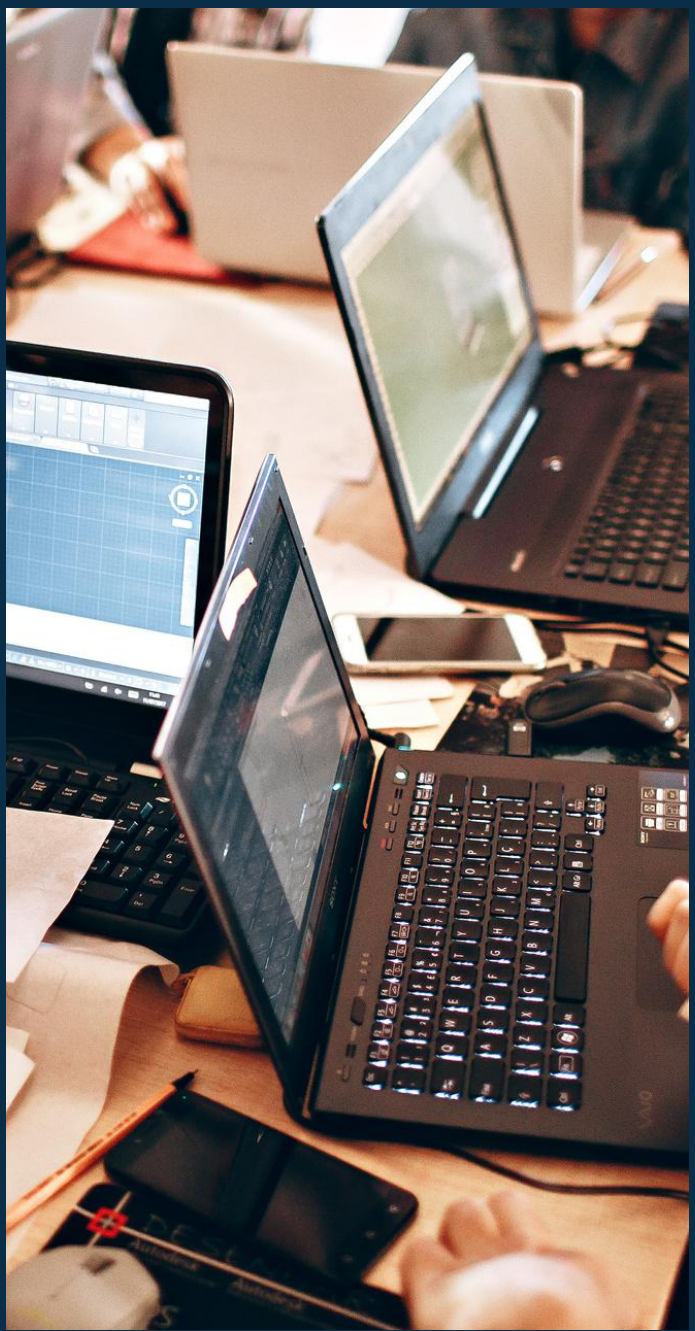
If you answered "yes" to two or more, it's probably time to upgrade.

CONTINUED – How Long Should Business Laptops Really Last?

How to Get the Most Out of Your Laptops
You can stretch the lifespan of your business laptops (while still keeping things running smoothly) with a few smart practices:

- Use business-grade laptops instead of consumer models.
- Install solid-state drives (SSDs) to boost speed.
- Perform regular maintenance (updates, malware scans, file cleanup).
- Join a hardware refresh cycle with your IT provider.
-

At LeadingIT, our **FleetComplete** leasing program includes automatic refreshes so you're never stuck with outdated hardware.



When Replacement Is Smarter Than Repair
We get it—replacing laptops can feel expensive. But holding onto old tech has hidden costs: lost productivity, more support tickets, and higher security risks.

A new laptop might cost $1,200. But if a slow laptop is costing an employee 15 minutes a day, that's **over 60 hours** of lost time per year.

Need Help Planning Your Next Laptop Upgrade?
If your team is constantly fighting with slow laptops or outdated tech, you're not alone — and you don't have to figure it out alone either.

At LeadingIT, we help businesses like yours make smart, stress-free decisions about when to upgrade and how to plan for it.

Let's chat for 15 minutes about your current setup — no pressure, no jargon, just real talk about what's working… and what's not.

Why We Enforce Cybersecurity Training: Protecting People, Data, and Business Continuity

Cybersecurity training might not generate headlines or boost sales, but make no mistake—it's one of the most cost-effective and high-impact investments an organization can make. According to a 2023 Tessian report, 90% of data breaches are caused by human error. This means that everyday mistakes like weak passwords or falling for a phishing scam can lead to massive financial loss or operational shutdown, so every employee plays a critical role in keeping the organization safe.

Cybersecurity training gives every team member the knowledge and confidence to spot risks before they become real problems.

Real Risk, Real Cost

Modern cyberattacks are no longer limited to complex code or brute-force hacking. Today's threats are highly targeted, relying on psychological tactics and social engineering. Phishing, for example, remains the most common and effective method of attack. In 2023 alone, Verizon's Data Breach Investigations Report found that 36% of breaches involved phishing. Even more concerning, many of these attacks don't require technical flaws, just one unsuspecting employee.

Take the Colonial Pipeline attack in 2021, where a single compromised password allowed attackers to access internal systems. The result was a ransomware shutdown of the largest fuel pipeline in the U.S., costing over $4.4 million in ransom alone and far more in supply chain disruption, lost productivity, and public fallout.

Situations like these are preventable. Cybersecurity training ensures your team knows how to spot and report suspicious activity before an incident escalates into a business crisis.

The Real Business Value

Cybersecurity directly supports key business outcomes:

1. Reduced Downtime: Cyber incidents often disrupt operations. Ransomware alone can halt business functions for days or even weeks. Training reduces the chances of these disruptions by minimizing the risk of breaches caused by human error.

2. Financial Savings: According to IBM's 2024 Cost of a Data Breach Report, the global average cost of a data breach is $4.88 million. Even a minor incident can lead to thousands in remediation, legal fees, customer notification requirements, and lost contracts. A well-trained workforce significantly lowers the likelihood and severity of those incidents.

3. Compliance and Liability: Most industries now require documented security awareness training as part of compliance (HIPAA, GDPR, PCI-DSS, etc.). Falling short can lead to fines or legal consequences. Regular training proves due diligence and supports audit readiness.

4. Customer Trust: Security-conscious organizations are more likely to earn and keep customer trust. When your team understands its security responsibilities, it builds confidence among partners, clients, and stakeholders.

5. Improved Cyber Insurance Eligibility and Rates: Many cyber insurance providers now factor employee training into coverage eligibility and premium pricing. Demonstrating a culture of security can lead to more favorable policy terms.

Conclusion: Security Training as a Business Strategy

Cybersecurity training is not a one-time event; it's an ongoing process. Threats evolve, and so must your team's knowledge. Ultimately, we enforce cybersecurity training not to check a compliance box, but to protect the people, data, and operations that keep your business running. The cost of not training your team is far greater than the time invested in learning.

What's a Patch, and Why Do We Keep Installing Them?

If you've ever been prompted to "install an update" or "restart to apply changes," you've encountered a patch. While it might seem like just another minor annoyance, especially when you're busy, patches are one of the most critical components of your organization's cybersecurity defense. Understanding what a patch is and why regular updates are non-negotiable can help protect your business from serious threats.

What Is a Patch?

A patch is a small piece of software developers issue to fix problems in existing programs. These problems might include bugs, functionality issues, or, most importantly, security vulnerabilities. Hackers actively search for flaws in software that they can exploit to gain unauthorized access to systems, steal data, or disrupt operations. Patches are the developers' way of sealing these digital cracks before attackers can use them.

Why Are Patches So Important?

Cybercriminals don't need to invent new methods to break into systems. They often use known vulnerabilities that haven't been patched. According to ServiceNow's 2024 research, 57% of data breaches could have been prevented simply by installing an available patch. In other words, the tools to stop many attacks already existed, but they weren't used.

Software updates and patches are essential because they:

- Fix security holes that hackers might use to access your network.
- Improve system stability, resolving crashes or glitches.
- Enhance performance by making software run more efficiently.
- Ensure compatibility with other new technologies or platforms.

Real-World Consequences of Skipping Patches

The 2017 WannaCry ransomware attack is a prime example of what can happen when patches are ignored. This global attack exploited a known Windows vulnerability for which Microsoft had already released a patch months earlier. Organizations that hadn't installed the patch fell victim, with hospitals, corporations, and governments facing locked files and multimillion-dollar damages.

Even today, hackers often scan the internet for devices running outdated software. Small businesses are especially vulnerable, as they may not have dedicated IT teams to monitor and apply updates regularly.

How to Stay on Top of Patching

You don't need a massive IT budget to manage patches effectively. Here are a few practical tips:

- Enable automatic updates for operating systems, browsers, antivirus programs, and key business software.
- Create a patch management schedule to regularly check systems that don't update automatically.
- Inventory your devices and software so you know what needs to be monitored.
- Educate employees to restart devices and install updates instead of postponing them.

Conclusion: Avoid the Risks

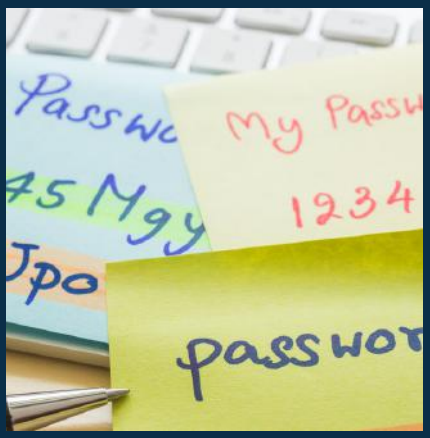
Timely patch management is a key part of any effective cybersecurity strategy. As cyber threats grow more sophisticated and frequent, failing to apply patches leaves your systems and business vulnerable to avoidable risks. At LeadingIT, we help organizations stay secure and compliant by implementing automated patching solutions and proactive monitoring. By keeping your systems current, we reduce your attack risk and ensure business continuity.

Cybersecurity on a Budget: What You Can't Afford Not to Do

Cybersecurity may seem like a luxury for organizations with deep pockets, but today's threat landscape doesn't discriminate based on budget. Small to mid-sized businesses are increasingly targeted by cybercriminals precisely because they often lack sophisticated defenses. Fortunately, robust cybersecurity doesn't always require a hefty price tag. By focusing on high-impact, low-cost strategies, organizations can significantly reduce their risk.

Here's what you can't afford not to do, regardless of your budget:

1. Prioritize Strong Password Hygiene



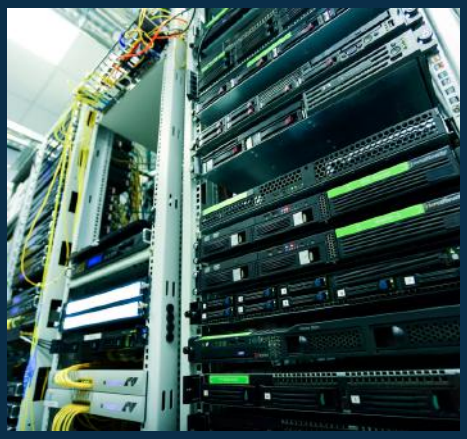
Weak or stolen passwords are involved in 81% of hacking-related breaches. One of the simplest yet most effective cybersecurity defenses is enforcing strong password policies. Encourage employees to use unique, complex passwords and enable multi-factor authentication (MFA) wherever possible. Consider using a reputable password manager to generate and store credentials securely. Many affordable or free options exist, making this an easy win for security.

2. Keep Software Updated

Outdated software is a favorite entry point for hackers. Regular patching of operating systems, browsers, and applications helps close known vulnerabilities. Enable automatic updates on all devices and establish a monthly check-in to verify nothing has fallen through the cracks. This proactive step requires no additional investment, just vigilance.

3. Train Your Staff

Human error continues to be one of the leading causes of cybersecurity breaches, accounting for 90% of incidents in 2023. Phishing emails, social engineering tactics, and malicious attachments can all compromise your network if employees aren't trained to spot red flags. Provide regular, bite-sized cybersecurity awareness training. Plenty of free resources are available from trusted sources like the Federal Trade Commission (FTC), Cybersecurity & Infrastructure Security Agency (CISA), and nonprofit organizations.



4. Back Up Your Data Consistently

Ransomware remains a major threat: 59% of organizations were hit by ransomware in 2024, with recovery costs averaging $2 million. A reliable backup strategy will save you time and money in the event of ransomware or data loss. Store backups both onsite and in the cloud, and test them periodically to ensure recovery is possible. Automated backup solutions are affordable and scalable, offering peace of mind without breaking the bank.

5. Secure Wi-Fi Networks and Devices

Ensure that your business Wi-Fi is encrypted, hidden, and protected by a strong password. Segregate guest and internal networks. On the device front, ensure all endpoints (laptops, smartphones, etc.) have antivirus software installed and use encrypted connections (VPNs) when accessing company data remotely.

6. Establish Clear Security Policies

Documented policies around acceptable use, remote work, device management, and data access help create a culture of accountability. They also clarify expectations for employees. While policy creation requires some upfront time, it costs nothing and can prevent confusion and risky behavior down the line.

Conclusion: Small Steps, Big Impact

Cybersecurity doesn't have to be expensive to be effective. The goal is to make your organization a harder target than others by eliminating the low-hanging fruit that hackers typically exploit. These foundational steps build cyber resilience and demonstrate a commitment to protecting your business, employees, and customers.

$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **$50** for every referral. If they sign up, you'll receive **$1000!**

SCAN TO LEARN MORE

815-788-6041 **GOLEADINGIT.COM/REFER**

DRIVEN – CHASES EXCELLENCE – HUMBLY CONFIDENT – ACCOUNTABLE – STAYS POSITIVE

LeadingIT Core Values Victor of the Month

James, Level 3 Lead Technician

Congratulations to this month's Values Victor for being Humbly Confident!

James shows us what it means to lead with quiet confidence. Whether he's tackling complex tech issues or mentoring others on the team, he approaches every challenge with skill, humility, and a willingness to learn. He doesn't pretend to have all the answers, but he knows how to find them. That's the power of staying curious, staying grounded, and never being afraid to ask for help when it counts.

Congrats, James!

LeadingIT

We Help Chicagoland Organizations Eliminate Concerns Over IT and Cybersecurity Where the Unsolvable is Solved with Unlimited Support, and an Unbeatable Guarantee.

WE ARE CELEBRATING!

BIRTHDAYS

JAMES CLAYTON	6/12
JEREMIAH BIRD	6/15
MIKE TARASIEWICZ	6/26

ANNIVERSARIES

MALLORY ROCHA	4 YEARS