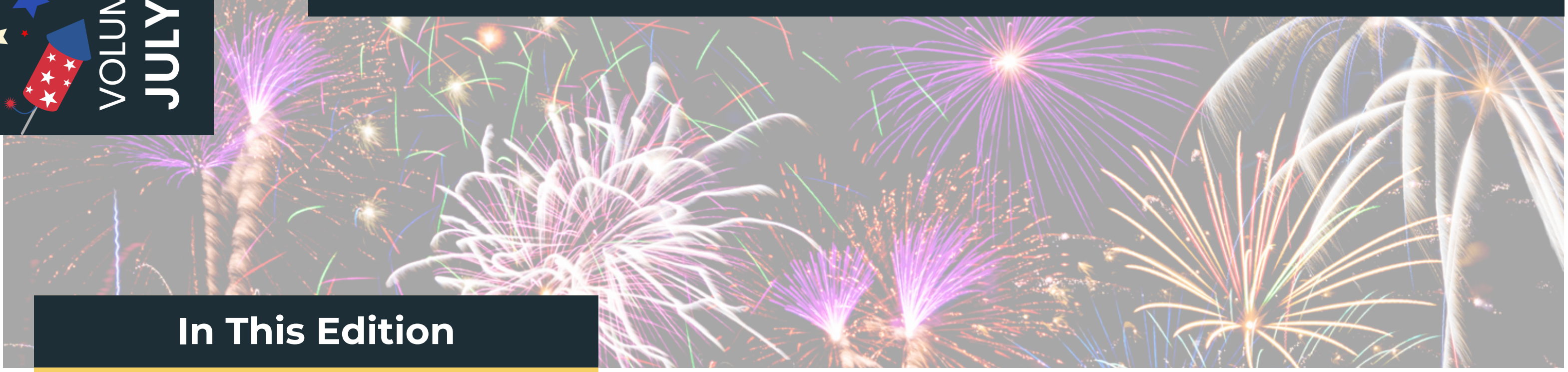
it's our word.
Loyality
TECH TALK

NEWSLETTER

VOLUME 24
JULY 2025



In This Edition

This monthly publication is provided courtesy of Kari Renn, President of LoyallTy.

OUR MISSION:

Our Mission: To make IT work at work so our clients can focus on their company goals without interruption.

7 Questions You Should Be Asking Your IT Provider Every Quarter (But Probably Aren't)

If you're only talking to your IT provider when you renew your contract, you're doing it wrong.

Technology isn't a "set it and forget it" part of your business. It's constantly evolving, and so are the threats that come with it. That's why quarterly IT check-ins are nonnegotiable if you want your business to stay protected, productive and competitive.

But here's the thing: Most business owners don't know what to ask.

So today, we're giving you a cheat sheet. These are the questions your IT provider should be ready to answer every single quarter – no tech-speak, no vague promises, just straight answers that keep your business running smoothly.

1. Are There Any Vulnerabilities We Need To Address Right Now?

This isn't just about checking boxes. You need to know:

- Is our antivirus up-to-date?
- Are there unpatched systems?
- Have we had any near misses or red flags lately?

You're not being paranoid – you're being prepared.

2. What's The Status Of Our Backups? And Have You Tested Them Lately?

Backups are like seat belts: You don't think about them until you really, really need them. Ask:

- When was the last time you tested a full restore?
- Are we using the right backup strategy? Off-site? Cloud? Hybrid?
- Are we backing up the right things?
- Is everything being backed up and stored securely?

You'd be shocked how many businesses think they're backed up…until they're not.

Continued on pg. 2

Continued from pg. 1

3. Are All Employees Following Security Best Practices?

It only takes one team member clicking the wrong link to bring the whole network down. Ask:

- Have there been any unusual logins or risky behavior?
- Do we need another round of phishing training?
- Are employees using multifactor authentication?

Bonus points if your IT provider brings this up before you ask. That's how you know they're watching.

4. How Has Our Network Performance Been? Anything Slowing Us Down?

Slow systems = slow teams = lost productivity (and money). Ask:

- Are there any recurring performance issues?
- Are we outgrowing our hardware or software?
- Is there anything we can optimize to speed things up?

Even small tweaks can make a big difference.

5. Are We Still Compliant With [HIPAA, PCI-DSS, GDPR, etc.]?

Regulations change. So do the rules about how you store and protect data. Ask:

- Are we meeting the standards for our industry?
- Have any requirements changed?
- Do we need to update policies, software or training?

Fines for noncompliance aren't cheap. Stay ahead of them.

6. What Should We Be Budgeting For Next Quarter?

Good IT is proactive. Ask:

- Are there any software licenses expiring?
- Any equipment nearing the end of its life?
- Any upcoming projects we should be planning for?

This helps you avoid surprise expenses and plan like a pro.

7. What Trends In IT Or Cybersecurity Are We Behind On That Are Making Us Slower Or More Vulnerable?

Technology doesn't stand still – and neither do cybercriminals. Ask your IT provider:

- Are there new tools or best practices we're not using yet?
- Are we lagging behind in any security protocols or performance benchmarks?
- What are other businesses our size doing that we're not?
- Are there any rising threats that we need to be more cautious of?

Falling behind on emerging trends doesn't just slow you down – it leaves you exposed. A great IT partner will keep you ahead of the curve, not playing catch-up.

You AREN'T Having These Conversations? Red Flag.

If your IT provider doesn't have clear answers to these questions – or worse, if they aren't offering to meet with you quarterly in the first place – you might not be getting the support you need.

Technology changes fast. Cyberthreats move faster.

You need someone who is not just reacting when something breaks but actively working to prevent the break in the first place.

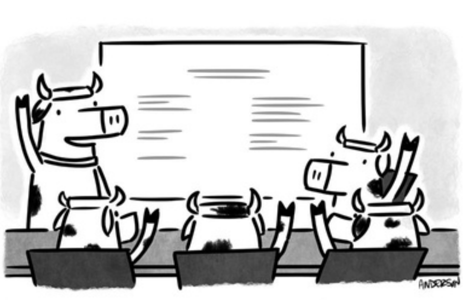
FREE CYBERSECURITY REPORT:

It's coming...

- That day a hacker steals critical data, rendering your office useless...
- That day when your bank account or credit card is compromised...
- Or that day when your customers' private lives are uprooted...

Download your free copy today and ensure you are prepared for any digital dilemma!

CARTOON OF THE MONTH



"Another unanimous vote! Man I love the herd mentality!"

The Hidden Costs Of Waiting: Why You Can't Afford To Delay Your Windows 10 Upgrade!

If you're still running Windows 10 on your business machines, let's cut to the chase: The clock is ticking.

On October 14, 2025, Microsoft is officially ending support for Windows 10. That means no more security patches, no more bug fixes and no more technical support.

But here's what business owners really need to understand: The cost of waiting isn't just about someday needing to upgrade.

It's about what waiting could cost you in the meantime.

"We'll Deal With It Later" Is An Expensive Strategy

We get it – upgrading every machine in your business isn't exactly your idea of a fun budget item. It feels easy to delay…until something breaks.

But here's what procrastination actually costs:

1. You're Operating Without A Safety Net

Once Microsoft discontinues Windows 10 updates, every new vulnerability becomes your responsibility.

Hackers love outdated systems because they're easy targets. It's like locking the front door but leaving the windows wide open.

One breach could cost you thousands – or worse, your entire business.

2. Software And Hardware Compatibility Issues

Many business apps, such as accounting tools, CRMs and industry-specific platforms, are already phasing out support for Windows 10.

If your systems stop working mid-project or crash during a client demo, what's that worth?

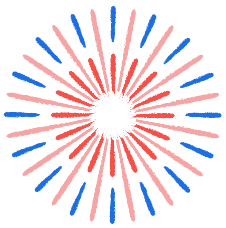
And it's not just software.

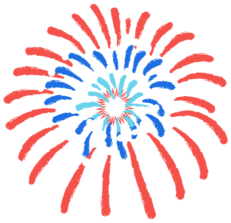
New printers, peripherals and even security tools may stop playing nicely with your outdated OS.

3. Lost Productivity

Outdated systems are slower, they crash more frequently and they frustrate your team. Even small lags add up over time, dragging down efficiency, morale and your ability to compete.

If every employee loses 10 to 15 minutes a day to tech hiccups, what does that cost you over a month?





4. Emergency Upgrades Are Always More Expensive

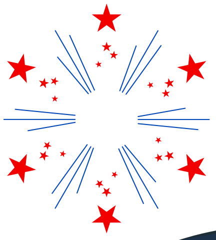
Waiting until your systems crash or your team is locked out doesn't just create stress – it creates panic-spend mode:

- Emergency hardware orders
- Rush IT labor fees
- Business interruptions while machines are replaced

A little planning now saves a lot of scrambling – and money – later.

5. You're Risking Compliance Violations

If your business handles sensitive data or is subject to regulations (HIPAA, PCI-DSS, etc.), using unsupported systems could result in fines or lawsuits. Many regulatory frameworks require up-to-date security – Windows 10 won't meet those standards come October.



Continued on pg. 4

Loyality it's our word.

REFERRAL PROGRAM

Recommend LoyalITy and get a $200 VISA for every qualified appointment booked.

LoyalITy will meet with your referral and determine if we are a good fit for their IT needs.

LoyalITy will propose a best-fit solution to solve their IT problems and concerns.

Your referral becomes a LoyalITy client - you get a $1,000 VISA!!

Continued from pg. 3

What Smart Business Owners Are Doing Now

They're getting ahead of the deadline, not just by upgrading devices, but by using this transition to:

- Audit what devices need to go
- Streamline tools and software
- Tighten up cybersecurity protections
- Plan smarter for IT spend in 2025

How To Make The Transition Smooth

Here's what we recommend:

- Run a compatibility check – Not all machines can run Windows 11. Find out which ones need to be replaced.
- Audit your apps – Make sure your essential tools are ready to run on Windows 11 or newer environments.
- Budget for hardware now – Don't get stuck in a supply chain crunch later.
- Partner with an IT provider – We can handle the transition from start to finish – no downtime, no surprises.

Don't Wait Until October To Panic

Waiting until the last minute will cost you more – in money, stress and missed opportunity. We're helping small businesses make the upgrade the smart way: planned, smooth and optimized for future growth.

Your Vacation Auto-Reply Might Be A Hacker's Favorite E-mail

You set it. You forget it. And just like that, while you're packing for vacation, your inbox starts broadcasting auto-reply messages to your co-workers. Harmless, right?

Actually, cybercriminals love these auto-replies. That simple message gives them valuable intel: your name, title, when you're unavailable, who to contact, internal team structure, and sometimes even travel details.

This provides two major advantages:

Timing – They know you're unavailable and less likely to catch suspicious activity.

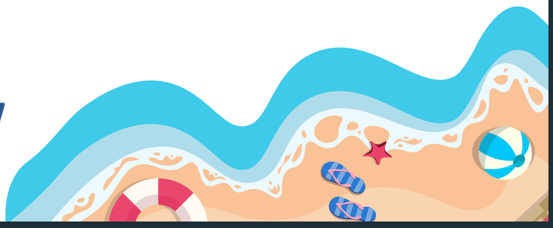
Targeting – They know who to impersonate and who to scam.

This sets the stage for a phishing or business e-mail compromise (BEC) attack.

How It Happens:

- Your auto-reply is sent.
- A hacker impersonates you or your alternate contact.
- They send an "urgent" request for money, passwords, or documents.
- A coworker, trusting the e-mail, complies.
- You return to discover fraud or a breach.

Businesses with traveling executives or sales teams are especially vulnerable. Admins often field many requests, handle sensitive tasks quickly, and may trust a well-crafted fake e-mail.



How To Protect Your Business:

1. Keep It Vague

Skip detailed itineraries. Instead, say: "I'm currently out of the office and will respond when I return. For immediate assistance, contact our main office at email@company.com."

2. Train Your Team

Educate staff never to act on urgent, sensitive requests based solely on e-mail. Always verify through another channel like a phone call.

3. Use E-mail Security Tools

Advanced filters, anti-spoofing protections, and domain monitoring reduce impersonation risks.

4. Enable MFA Everywhere

Multifactor authentication across all accounts blocks hackers even if passwords are compromised.

5. Partner With A Proactive IT Provider

An experienced cybersecurity team can detect suspicious activity early and stop attacks before they cause serious damage.

Ready to take your IT to the Next Level?

Scan the QR code and book a 30 Minute Discovery Call with us to learn about what we can do for your IT!