August 2025

TechTidbit.com

brought to you by Tech Experts

Building A Smart Data Retention Policy: What Your Small Business Needs To Keep (And Delete)

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Running a business today means juggling more data than ever.

Employee files, vendor contracts, financial records, customer emails, and all those back-up files - they pile up quickly. And unless you have a system in place to manage all that information, it can start to feel overwhelming fast.

In fact, a recent study found that nearly three-quarters of business leaders have delayed or avoided making decisions simply because the data felt too overwhelming to sort through. That's a lot of missed opportunities and wasted time.

The solution? A clear, practical data retention policy. It doesn't have to be complicated, but it does need to be consistent. At its core, a good retention policy helps you figure out what data to keep, what can be safely deleted, and when it's time to make that call. And it's not just about cleaning house - it's about protecting your business, reducing risk, and saving money.

Why is this important? For starters, there are compliance rules - both local and industry - specific-that require certain documents and records to be retained for a set number of years.

If you're ever audited or involved in a legal dispute, having the right information available (and easily accessible) can make a huge difference.

Then there's security. Storing everything forever might seem harmless, but old data can become a liability. The more information you hold onto, the more attractive your systems become to hackers - and the harder it is to protect everything properly.

Organizing your digital files and archiving or deleting what you no longer need is a smart way to reduce risk.

It also makes your systems faster and easier to manage. Imagine trying to run your business with a file cabinet stuffed full of every document you've ever handled. It's no different in the digital world. Removing outdated or unnecessary files frees up space, improves performance, and makes it easier to find the data you need day to day.

Creating a data retention policy starts with understanding what kinds of data your business creates and where it all lives - on servers, in cloud apps, in email inboxes, and maybe even on individual computers. Once you know that, you can start to decide how long each type of information should be kept, who's responsible for managing it, and what happens to it over time.

You don't need to go it alone, either. There are tools that can help automate the process and professionals (like us) who can help guide you through it.

Think of your data like your office closet - if you never clean it out, eventually you won't be able to find anything. A well-thought-out retention policy turns digital clutter into a well-organized, secure, and compliant information system that supports your business instead of slowing it down.

Ready to get started? Let's put a plan in place to take control of your digital records before they start controlling you.

Storing everything forever might seem harmless, but old data can become a liability. The more information you hold onto, the more attractive your systems become to hackers - and the harder it is to protect everything properly.

Could Social Engineering Bring Down Your Business?

"It often starts with a phone call or email from someone pretending to be a colleague, a supplier, or even a senior manager. They might sound friendly, urgent, or frustrated... anything to get the response they want."

One phone call could be all it takes to bring your business to its knees.

That's the chilling reality of social engineering. It's a type of cyberattack that doesn't rely on clever coding or fancy tech. Instead, it targets your people. And it's becoming one of the biggest threats to businesses of all sizes.

Social engineering is when a criminal manipulates someone into giving up sensitive information or access to systems.

It often starts with a phone call or email from someone pretending to be a colleague, a supplier, or even a senior manager. They might sound friendly, urgent, or frustrated... anything to get the response they want.

And if your staff aren't on high alert, that one conversation could open the door to your entire network.

A favorite target for these attacks? Your customer service team. They're trained to be helpful and solve problems quickly.

But if someone calls pretending to be locked out of their account and urgently needs a password reset, it's easy to see how a well-meaning team member could be tricked into handing over access.

From there, it's game over. Attackers can install ransomware, steal customer data, or snoop around in your systems undetected.

The worst part is this kind of attack is simple to pull off. And highly effective. That's why even small businesses need to take it seriously.

So, what can you do?

Start by training your team to be cautious of unusual requests, even if they sound legitimate. And don't rely on memory or gut instinct. Put strong identity verification procedures in place that everyone follows, every time. Technology can help with this by adding extra checks before any sensitive action is taken.

Remember, cybercriminals don't need to break in when someone will open the door for them. But with the right awareness and safeguards, you can make sure your team knows how to keep it firmly shut.

Need help keeping your team on top of cybersecurity best practices? Get in touch.

We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Don't Let Outdated Tech Slow You Down: Build A Smart IT Refresh Plan

Nothing throws off your day like a frozen screen or a sluggish computer. If you run a small business, you've probably dealt with outdated tech more than once. Sure, squeezing extra life out of old equipment feels economical, but it often costs more in the long run.

Small businesses lose approximately 98 hours per year, equivalent to 12 working days, due to technology concerns such as slow PCs and outdated laptops.

That's why having an IT refresh plan matters. It keeps your team running smoothly, avoids unexpected breakdowns, and helps you stay secure.

Regardless of whether you outsource managed IT services or handle them in-house, a solid refresh strategy can save time, stress, and money down the line.

Why having a strategy in place is important

It's easy to ignore old hardware until something breaks. But when things start falling apart, you have no choice but to look for better parts, deal with downtime, or even explain to your team and clients why things are slow.

The risks of not planning include:

- Unexpected downtime: even one broken laptop can stop an entire day of work.
- Productivity tanks: Outdated tech runs slower, crashes more often, and just can't keep up.
- Security risks go up: Older systems miss out on key updates, leaving you exposed.
- Compliance issues: Especially if your business needs to meet certain tech standards or regulations.

A little planning now can save you from a lot of headaches later.

Four simple strategies for a smart refresh plan

Replace as you go. Instead of replacing everything all at once, swap out equipment gradually. When a machine starts acting up or hits the end of its lifecycle, replace it.

Your IT support provider can help you set a realistic "expiration date" for each device. This approach spreads out the costs and keeps surprises to a minimum.

Schedule regular refresh cycles. If your team relies heavily on tech or you'd rather not wait for things to go wrong, consider refreshing your hardware on a set schedule. It's a cleaner, more predictable way to keep your tech current and makes budgeting easier.

Watch for compatibility issues. Tech doesn't exist in a vacuum. Waiting until something breaks or no longer works with your tools, puts your business in panic mode. Have your IT partner do regular checkups to make sure your equipment still plays nice with your software.

Don't be afraid of leasing. If big upfront costs are holding you back, leasing might be worth a look. Many IT vendors offer lease options with flexible terms. If your company's refresh cycle is every four years, for example, a four year lease makes sense. It's a way to get the latest gear without blowing your budget all at once.

What to do next

1. Take inventory: Write down what you've got and how old it is.
2. Set your goals: Your refresh plan should support where your business is headed.
3. Talk to your IT services provider: They can help you figure out the best timing, budget, and options.
4. Create a simple schedule: A plan is better than winging it.

Stay ahead by refreshing smart

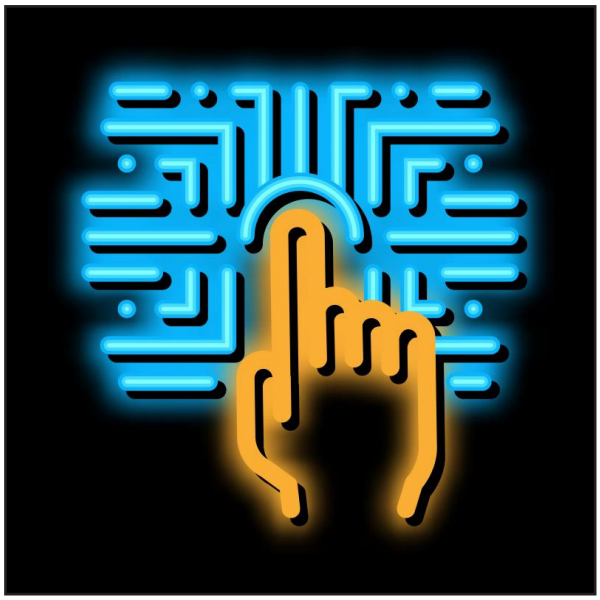
A good IT refresh strategy protects productivity, improves security, and future-proofs your business. Need help building yours? Contact us today at info@mytechexperts.com, or (734) 457-5000.

"It's easy to ignore old hardware until something breaks. But when things start falling apart, you have no choice but to look for better parts, deal with downtime, or even explain to your team and clients why things are slow."

Biometrics Are the New Password - But What Happens If Yours Gets Stolen?

Technology moves fast, and one area that's quickly becoming part of everyday business life is biometrics. Instead of typing in a password, more people are logging in with a fingerprint, a facial scan, or even voice recognition. It's quick, easy, and it feels more secure. No more forgotten passwords or sticky notes under keyboards.

But as with most things in technology, convenience comes with a catch.



Unlike a password, you can't change your fingerprint. You can't "reset" your face. So if your biometric data is compromised, it's not just a minor headache - it's potentially a long-term problem.

And that has business owners starting to take a second look at how this data is being used and protected.

Biometric information is now among the most valuable types of data a business can hold. That makes it a prime target for hackers. If your systems store fingerprint or facial data - especially if you're using it for employee or client logins - you've got to treat that data like gold.

Unfortunately, cybercriminals already know how powerful biometric credentials are. Unlike a password that can be changed in minutes, biometric data is permanent. That's part of what makes it so attractive to attackers.

On underground markets, this type of information is sold at a premium. Criminals can use it to get past identity checks, access systems, and even impersonate someone online.

So what's the best way to protect your business? The first step is understanding where and how this data is stored. If you're using devices that store biometric information locally - such as a smartphone or a fingerprint reader on a laptop - that's often safer than storing it in a central database.

Local storage keeps the data off the network, which makes it harder for hackers to get to.

However, if you do need to store biometric data on a server - maybe for time tracking, door access, or centralized logins - it needs to be properly secured.

That means strong encryption, keeping it separate from other sensitive data, and limiting who has access to it. You'll also want to monitor and log any changes or login attempts.

If you're using third-party apps or devices that rely on biometric login, make sure you know how those vendors handle security. Read the privacy policy, ask questions, and check whether they've had any past data breaches.

Not all providers treat this data with the care it deserves, and you don't want to find that out the hard way.

Done right, biometrics can be a great tool. They streamline access, make logins easier, and reduce password fatigue for your team. But they need to be handled with the same (or even more) care than a traditional password system.

Bottom line: If you're going to use something as personal as a fingerprint or a face scan to unlock your business systems, make sure you're the only one with the key.

Want help reviewing your current biometric security practices? We're happy to chat. Reach out today.

Contact Information

Tech Experts Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com