February 2026

TechTidbit.com

brought to you by Tech Experts

Cyber Resilience Matters More Than You Think

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

Most businesses still picture cybersecurity like an old-school castle. Tall stone walls. Heavy iron gates. A moat full of alligators, if possible.

The idea is simple: keep the bad guys out, and everything inside stays safe.

That model made sense once. But it doesn't anymore.

Today's workplace isn't a castle. Your employees work from home, the office, hotels, and coffee shops. Your data lives in the cloud. Your systems connect to dozens of outside vendors, apps, and services every day. Files are shared constantly. Logins happen from everywhere.

There is no single wall to defend anymore, and cybercriminals know it.

That's why the focus of cybersecurity has quietly shifted over the last few years. It's no longer just about trying to block every possible attack. It's about assuming something will eventually get through, and making sure your business can recover quickly when it does. That mindset is called cyber resilience.

Frankly, even well-protected organizations get hit. Someone clicks the wrong link. A trusted supplier suffers a breach. A password gets reused. A convincing, AI-powered scam slips past email filters. It happens to smart, careful companies every single day.

The difference between a crisis and a minor disruption is what happens next.

A cyber-resilient business is built to spot trouble early, contain it quickly, and recover without chaos. Instead of panic, finger-pointing, and downtime, the response is calm and methodical. Accounts get locked down. Systems are isolated. Data is restored. Business resumes. That doesn't happen by accident.

One major piece of cyber resilience is visibility - having systems that constantly watch for unusual behavior, not just obvious "alarms." Modern security tools look for things like strange login locations, unusual file access, or activity that doesn't match a user's normal pattern. Many of these tools now use AI to spot problems long before a human ever would.

This is important because today's attacks often don't announce themselves. Hackers don't always smash windows. More often, they log in quietly and try to blend in.

Then there's the safety net: backups.

Not just "we think we have backups," but properly designed, secure, and tamper-proof backups that attackers can't delete or encrypt. When backups are set up correctly, recovery can be surprisingly fast. In some cases, systems are restored so quickly that customers never even realize something went wrong.

But technology alone isn't enough.

Cyber resilience also depends on people. Employees need to recognize suspicious emails and feel comfortable reporting mistakes immediately.

Leadership needs a simple, clear plan for who does what when something goes wrong. Everyone needs to understand that speaking up early is always better than staying quiet and hoping a problem disappears.

Cyber resilience is about preparation and accepting reality, staying calm under pressure, and having the ability to bounce back quickly when the unexpected happens.

If your business hasn't thought beyond "keeping the bad guys out," it may be time to rethink your approach.

And if you'd like help building a practical cyber resilience strategy that fits how your business actually operates, we're here to help.

A cyber-resilient business is built to spot trouble early, contain it quickly, and recover without chaos. Instead of panic, finger-pointing, and downtime, the response is calm and methodical. Accounts get locked down. Systems are isolated. Data is restored. Business resumes. That doesn't happen by accident.

Hackers Aren't Hacking - They're Just Logging In

"Once attackers log in, they take their time. They read emails. They learn how invoices are sent. They figure out who approves payments. Then they strike."

When most business owners picture a cyberattack, they imagine a hoodie-wearing genius furiously typing code, breaking through firewalls, and "hacking" their way into a network.

That image is outdated.

Today's cybercriminals usually aren't hacking anything at all. They're logging in - using real usernames and real passwords.

And that's what makes modern cybercrime so dangerous. Attackers have figured out that breaking in is hard. Logging in is easy.

Instead of trying to defeat security systems, they steal or buy login credentials and walk right through the front door. Once inside, they look exactly like a normal employee.

Your systems don't raise alarms because, technically, nothing unusual is happening. This shift has changed the rules of the game.

How Do Hackers Get Logins?

Most of the time, it starts outside your business. Employees reuse passwords across multiple websites. A breach at a social media platform, online retailer, or personal email account exposes those passwords. Criminals collect them, bundle them together, and sell them on underground marketplaces.

From there, automated tools try those same email-and-password combinations against business systems like Microsoft 365, Google Workspace, VPNs, and remote access portals.

If one works, they're in. No malware. No warning pop-ups. No dramatic breach notification. Just access.

Why Small Businesses Are Prime Targets

Large companies make headlines, but small businesses are easier and more profitable targets.

Smaller organizations often assume they're "too small to bother with." Attackers know better.

They know smaller businesses tend to have weaker security, fewer safeguards, and limited monitoring.

Even more appealing: small businesses often serve larger ones. Law firms, accountants, manufacturers, contractors, medical offices - these are gateways to valuable data and trusted relationships.

Once attackers log in, they take their time. They read emails. They learn how invoices are sent. They figure out who approves payments. Then they strike.

That's how wire fraud happens. That's how fake invoices get paid. That's how ransomware spreads quietly before detonating.

Why Passwords Alone No Longer Work

Passwords used to be enough. They aren't anymore.

Even strong passwords fail if they're reused or stolen somewhere else.

You can do everything "right" internally and still get compromised because the password was exposed on an unrelated site years ago.

That's why breaches today often leave business owners stunned.

"We didn't click anything."

"We didn't download anything."

"Our antivirus never went off."

All true - and all irrelevant. The attacker didn't force their way in. They logged in.

The One Control That Stops Most Attacks

There's a simple reason cybersecurity professionals push so hard for multi-factor authentication (MFA). It works.

MFA requires something you know (your password) and something you have (a phone app, text code, or hardware key). Even if a criminal has the password, they can't complete the login without the second step.

It's not flashy. It doesn't feel dramatic. But it stops the vast majority of account-based attacks cold.

When businesses skip MFA because it's "inconvenient," they're betting the company on convenience.

That's rarely a good trade.

What Business Owners Should Take Away

Cybersecurity today isn't about fighting hackers in dark basements. It's about controlling access. Ask yourself a few simple questions:

Could someone log in as one of my employees from another country?

Are email, remote access, and cloud systems protected with MFA?

Would we even notice if someone quietly accessed our systems today?

If the answers aren't clear, that's a risk - not a technical problem, but a business one.

Hackers aren't breaking in anymore. They're logging in.

And the businesses that recognize that reality are the ones staying ahead of the next incident, instead of reacting after the damage is done.

The "Deepfake CEO" Scam: Voice Cloning Is The Next Cyber Threat

The phone rings, and it's your boss. The voice is unmistakable; with the same flow and tone you've come to expect. They're asking for a favor: an urgent wire transfer to lock in a new vendor contract or maybe sensitive client information that's strictly confidential.

Everything about the call feels normal, and your trust kicks in immediately. It's hard to say no to your boss, and so you begin to act.

What if this isn't really your boss on the other end? What if every inflection, every word you think you recognize has been perfectly mimicked by a cybercriminal?

In seconds, a routine call could turn into a costly mistake; money gone, data compromised, and consequences that ripple far beyond the office.

What was once the stuff of science fiction is now a real threat for businesses. Cybercriminals have moved beyond poorly written phishing emails to sophisticated AI voice cloning scams, signaling a new and alarming evolution in corporate fraud.

How AI voice cloning changes the threat landscape

We have spent years learning how to spot suspicious emails by looking for misspelled domains, odd grammar, and unsolicited attachments. Yet we haven't trained our ears to question the voices of people we know, and that's exactly what AI voice cloning scams exploit.

Attackers only need a few seconds of audio to replicate a person's voice, and they can easily acquire this from press releases, news interviews, presentations, and social media posts

A scammer doesn't need to be a programming expert to impersonate your CEO. They only need a recording and a script.

Traditionally, business email compromise (BEC) involved compromising a legitimate email account through techniques like phishing and spoofing a domain to trick employees into sending money or confidential information. BEC scams relied heavily on text-based deception, which could be easily countered using email and spam filters.

While these attacks are still prevalent, they are becoming harder to pull off as email filters improve.

Voice cloning, however, lowers your guard by adding a touch of urgency and trust that emails cannot match.

"Vishing" (voice phishing) uses AI voice cloning to bypass the various technical safeguards built around email and even voice-based verification systems. Attackers target the human element directly by creating high-pressure situations where the victim feels they must act fast to save the day.

Challenges in audio deepfake detection

Few tools currently exist for real-time audio deepfake detection, and human ears are unreliable as the brain often fills in gaps to make sense of what we hear.

That said, there are some common tell-tale signs, such as the voice sounding slightly robotic or having digital artifacts when saying complex words. Other subtle signs you can listen for include unnatural breathing patterns, weird background noise, or personal cues such as how a particular person greets you.

Securing your company against synthetic threats

As AI tools become multimodal, we will likely see real-time video deepfakes joining these voice scams, and you will need to know how to prove that a recording is false to the press and public.

Waiting until an incident occurs means you will already be too late.

Does your organization have the right protocols to stop a deepfake attack? Contact us today to assess your vulnerabilities and secure your communications against the next generation of fraud.

"What was once the stuff of science fiction is now a real threat for businesses. Cybercriminals have moved beyond poorly written phishing emails to sophisticated AI voice cloning scams, signaling a new and alarming evolution in corporate fraud."

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.

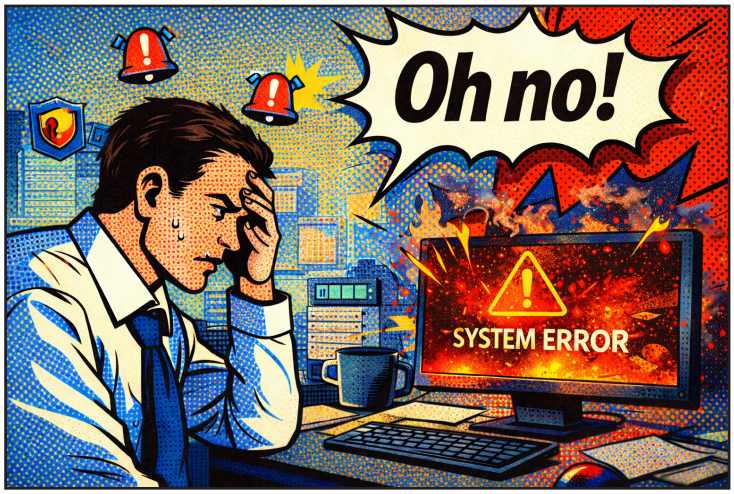
Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Why "It Hasn't Happened To Us (Yet!)" Is The Most Expensive IT Strategy

There's a small word people usually leave off the end of this sentence: "It hasn't happened to us… yet."

Most business owners don't say the word out loud, but it's always there. Unspoken. Understood.

The systems are running. Email works. Files open. No one has locked up the network. No clients are calling about strange messages. So it feels safe to assume that whatever happens to other companies probably won't happen here.



At least not anytime soon.

The problem isn't that this thinking is reckless. It's that it quietly assumes time is on your side.

Technology doesn't usually fail in dramatic, movie-style fashion. It fails slowly, silently, and then all at once. Settings drift. Hardware ages. Security tools fall behind. Backups run without ever being tested. One workaround turns into a permanent solution because everyone is busy.

Nothing breaks, so nothing changes. That "yet" keeps getting pushed forward.

Then something ordinary happens on an ordinary day. A password is reused. A software update doesn't go as planned. An employee clicks a link they've clicked a hundred times before. A server that's been "fine for years" finally isn't.

And suddenly the question becomes: Why are we dealing with this now?

The answer is almost always the same. It didn't happen earlier, but it was always going to happen eventually.

For small and mid-sized businesses, the cost isn't just the technical repair. That part is usually solvable. The real damage comes from everything that stacks up around it.

Work stops. Deadlines slip. Employees wait. Customers notice. Leadership gets dragged into decisions they shouldn't be making in the middle of the day. People scramble without a plan because the plan was "we'll deal with it if it ever comes up."

The "yet" has arrived. What surprises most owners is how long the fallout lingers. Productivity doesn't snap back instantly. Systems behave oddly for weeks. Data has to be verified. Trust has to be rebuilt - internally and sometimes externally. Everyone remembers how fragile things felt.

None of this happens because someone ignored a warning labeled "Disaster Ahead." It happens because everything appeared stable enough to postpone improvements one more quarter, one more year, one more budget cycle.

Businesses that avoid this trap don't do it by being paranoid. They do it by being realistic.

They assume failures will happen eventually and plan accordingly. They design environments that are predictable, documented, and recoverable. They test the things they hope they'll never need. They remove single points of failure before those points get to choose the timing.

They don't rely on luck as a business strategy. "It hasn't happened to us yet" is a comforting thought. It feels responsible. It feels measured.

But "yet" is doing more work than most people realize.

And when that word finally cashes in, it usually does so at the worst possible time - and at a much higher cost than anyone expected.

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