frogworks

June 2026

Issue 06 Volume 16

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

- The Security Blind Spots Putting Small Business at Risk

The Security Blind Spots Putting Small Businesses at Risk

When you think about protecting valuable assets, you probably think about physical security, with locks, guards, vaults, and surveillance. Companies spend big bucks keeping their buildings safe, but even with all that protection, defenses are only as strong as their weakest link.

The same holds for small business security risks, where perimeter defenses alone rarely tell the whole story. Many owners focus on the obvious "front doors" like firewalls and antivirus software, but ignore the hidden vulnerabilities inside that let threats roam free.

Why "Fortress Mentality" Leaves You Exposed

Attackers know small businesses handle customer data, financials, and operations. They also know that small companies don't protect those assets as well. The result? Blind spots like unmonitored internal traffic, where threats can hide after sneaking past the perimeter.

That's why addressing small business security gaps requires looking beyond who is allowed in and paying attention to what happens next. If unusual behavior goes unnoticed, damage can spread long before alarms go off.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

The Security Blind Spots Putting Small Businesses at Risk

The Sneaky Internal Threats No One Talks About

In most cases, once a hacker gains access to your network, they move laterally, quietly stealing data or planting ransomware. Without visibility inside your network, these movements go unnoticed because they blend in with normal activity.

Mitigating network visibility risks isn't as complicated as it sounds. Tools that monitor east-west traffic (i.e., data moving between devices within your network) can flag unusual patterns, such as a workstation suddenly accessing sensitive files it has never accessed before.

Eliminating internal network blind spots means monitoring traffic between systems, users, and devices. Without visibility into internal activity, it's easy to miss signs, such as unauthorized file access, odd login times, or data moving where it shouldn't.

Overlooked Spots in Everyday Operations

Your IT service desk might be another weak link. A convincing phone call or email can lead to password resets or access approvals that should not happen. And if tickets pile up or issues go unresolved, it creates opportunities for social engineering attacks.

Other common small business security risks? Outdated software, shadow IT, and poor backup testing. These aren't flashy threats, but they quietly erode your defenses.

Simple Steps to Secure Your Business

Cybersecurity doesn't have to keep you up at night. By addressing small business security gaps like internal blind spots and adopting proactive cybersecurity for SMBs, you turn your operation into a true fortress.

Start by implementing multi-factor authentication everywhere and securing IT service desks with better protocols, training, verification procedures, and limited permissions. Train your team regularly to spot phishing attempts and patch systems promptly. But don't stop at the perimeter. Add internal network monitoring to catch threats early. Partnering with a managed service provider offers deep visibility without overwhelming your team.

A proactive approach to cybersecurity lets you respond early rather than clean up after a breach. Early detection often means lower costs, less downtime, and fewer reputational headaches.

Turning Awareness Into Action

The most secure organizations know that proper protection goes beyond locked doors. Proactively strengthening internal visibility helps you better protect what matters most and reduce small business security risks before they turn into costly breaches.

Hidden Technology Barriers Crippling Small Businesses

When business owners talk about growth, technology is often part of the plan. However, it's not always part of reality.

Have you invested in a new system, platform, or AI tool expecting instant results, only to feel stalled months after signing the contract? In practice, these technology challenges for small businesses are rarely an issue with the tools themselves. More often, the real obstacles are outdated systems or team resistance that lead to rework, delays, and missed deadlines.

What's Really Causing the AI Adoption Gap?

Many business owners find themselves excited about a tool that could streamline operations, only to have doubts creep in mid-rollout. Will the team embrace it or push back, or will this be a massive waste of time?

This apprehension is the biggest barrier to adopting AI. Leaders struggle to separate real ROI from hype, while middle managers worry automation will expose inefficiencies. Employees, meanwhile, fear being left behind without a clear path to reskill.

Without trust and a practical roadmap to adoption, even the most promising tools will sit unused. Addressing small business technology barriers starts with communication, training, and realistic expectations.

When Legacy Systems Turn Into Silent Killers

Another technology challenge for small businesses is identifying internal technical debt, or old setups you've patched together over the years. Improving information technology infrastructure sounds straightforward, but integrating new stuff with "messy legacy systems" creates gridlock.

For smaller operations, this plays out in everyday frustrations that slow progress: software that doesn't communicate, slow computers thwarting growth, or security gaps you didn't even know existed.

Technology most often fails because misalignment between leadership, IT, and operations undermines progress. For small businesses, mitigating operational technology risks means getting everyone on the same page before signing contracts and draining budgets.

Identifying internal technical debt requires an honest audit of existing systems. If staff rely on spreadsheets to fix gaps in core software, that's a red flag. Improving information technology infrastructure doesn't always mean replacing everything. It often means simplifying, integrating, and cleaning up what's already there.

Hidden Technology Barriers Crippling Small Businesses

Start Overcoming Hidden IT Challenges

The good news? Overcoming hidden IT challenges doesn't require a massive overhaul. Start small by:

- Auditing your current setup to determine what's working and what's dragging you down
- Involving your team early; get their input to build buy-in.
- Prioritizing quick wins, like cloud tools that integrate easily.
- Focusing on training and clear communication to ease fears.

Addressing these issues doesn't require perfection; it requires focus. Start by choosing one process that would benefit from automation. Set measurable goals, involve the people who actually use the system, and invest in training alongside technology.

Clear ownership also matters. When no one is accountable for implementation, tools stall. Assign a project lead who can bridge the gap between business needs and technical realities.

Technology Should Work for You

Technology should reduce friction, not add to it. By proactively tackling fear, legacy issues, and risks, you'll turn potential roadblocks into real advantages. The most successful organizations understand that technology challenges for small businesses are as much about people and processes as they are about software.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter