frogworks

July 2026

Issue 07 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 Hidden Cybercrime Draining Your Paycheck

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

Get More Free Tips, Tools, and Services At Our Web Site: www.GetFrogworks.com
Or call: (240) 880-1944

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.

The Hidden Cybercrime Draining Your Paycheck

If you sign off on payroll every few weeks, you probably feel confident that the money is going where it's supposed to go.

However, many business owners don't realize that payroll fraud is a real problem. Okta's latest threat intelligence shows that payroll fraud is quietly becoming one of the most profitable cybercrimes targeting everyday businesses.

When bonuses, commissions, and holiday paychecks are in motion, attackers see opportunity. Instead of locking systems or causing noticeable damage, criminals slip in and redirect money before anyone notices.

Why Payroll Is a Goldmine for Cybercriminals Right Now

Cybercriminals follow the money, and payroll is predictable, recurring, and trusted. However, because most people would notice a significant change to their weekly pay, payroll diversion fraud and direct deposit hijacking often target holiday bonuses.

Instead of blasting thousands of phishing emails or dropping ransomware, these surgical attacks target one or two employees (usually higher-paid ones) and quietly change the direct deposit routing on their paycheck. Once they make the switch, the employee's pay is deposited into the attacker's account.

But how do the hackers get access to employee accounts? In most cases, they simply call or email the help desk pretending to be the employee. They already have a few pieces of personal information (usually scraped from LinkedIn, data breaches, or social media), claim they're locked out of the benefits portal, and beg for a quick password reset or a change to direct deposit.

Because the request sounds urgent and happens during the holiday rush, many support teams approve it without following the standard verification process.

Why Traditional Security Tools Miss These Attacks

Firewalls and endpoint protection do very little to prevent most payroll diversion fraud protection failures. These attacks exploit trust, process gaps, and rushed approvals. From a system perspective, everything looks legitimate.

Payroll changes submitted through proper channels rarely raise alarms. That is what makes payroll fraud so difficult to detect until an employee reports missing pay. By then, recovery is often slow and incomplete.

The Hidden Cybercrime Draining Your Paycheck

Simple Steps To Reduce Payroll Risk

Workplace cybersecurity and payroll safety depend on process discipline, not just technology. Businesses can reduce exposure to holiday bonus phishing scams with a few practical controls:

- Require multi-step verification for any payroll or direct deposit change.
- Separate payroll approval duties so no single person can authorize changes alone.
- Delay payroll change requests before bonus cycles to allow extra review time.
- Train HR and help desk staff to recognize employee help desk social engineering tactics.
- Encourage employees to verify changes directly through known internal contacts.

These steps are inexpensive and effective.

Payroll Fraud Isn't Going Away, But You Can Make It Much Harder

Payroll fraud through diversion and employee help desk social engineering thrives because it's low-risk and high-reward for attackers. The good news? Most successful attacks rely on bypassing basic human verification steps that you can tighten today.

Take a few minutes this week to review your change-of-banking procedures and talk to your team about staying extra cautious during the holiday bonus season. Direct deposit hijacking awareness and workplace cybersecurity and payroll safety discipline now can save you (and your employees) from a costly January surprise.

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