RISK ADVISORY · SMB SECURITY

5 hidden IT risks that could shut down your business in 2026

The biggest risks this year aren't obvious. They're hidden inside everyday tools, user behavior, and outdated assumptions.

WRITTEN BY
Pascal Eggers, Rhodian Group

TOPIC
Cybersecurity & IT Risk

READ TIME
6 minutes

Most small and mid-sized businesses believe they're "covered" when it comes to IT and cybersecurity.

You've got antivirus.
You've got backups.
Maybe even multi-factor authentication.

So you're safe… right?

Not anymore.

At Rhodian, we work with businesses every day that felt the same way — until gaps in their environment were exposed. Here are the five most overlooked IT risks we see, and where we help close them.

RISK 01

Identity attacks: your new #1 threat

For years, cybersecurity focused on protecting the network perimeter — firewalls, antivirus, endpoint protection. That's no longer where most of the battle is being fought. Today, attackers are going straight after **user identities**.

> WHAT MOST BUSINESSES THINK
>
> *"We turned on MFA, so we're secure."*

WHAT'S ACTUALLY HAPPENING

- Attackers use **MFA fatigue attacks**, bombarding users with login prompts until one gets approved
- Stolen **session tokens and browser cookies** can bypass MFA entirely
- Compromised accounts look like legitimate users, making them far harder to detect

Industry trends show security shifting heavily toward identity and access risk, not perimeter defenses.

WHY IT MATTERS

If an attacker gets into a user account, they can access email and sensitive data, launch internal phishing attacks, and move laterally across your environment — all without triggering traditional alerts.

HOW RHODIAN HELPS

We go beyond basic MFA by implementing:

- Conditional Access policies
- Device-based access controls
- Identity monitoring and anomaly detection

The goal isn't just login protection — it's continuous identity security.

RISK 02

Unmanaged devices accessing your business data

Hybrid work isn't going away — but it comes with hidden risks.

> WHAT MOST BUSINESSES THINK
>
> *"Employees occasionally use personal devices — it's no big deal."*

WHAT'S ACTUALLY HAPPENING

- Personal devices often lack security patches, endpoint protection, and monitoring tools
- Sensitive data is accessed through browsers and cloud apps, outside your visibility

WHY IT MATTERS

This creates a massive blind spot:

- Data can be downloaded or shared outside your control
- Malware on a personal device can reach business systems
- Compliance risk increases dramatically

HOW RHODIAN HELPS

We implement:

- Zero Trust access controls
- Device compliance enforcement
- Secure remote access policies

Only trusted users on trusted devices get access — no exceptions.

RISK 03

SaaS sprawl (you don't know what you're using)

Most businesses underestimate how many applications they actually use.

> WHAT MOST BUSINESSES THINK
>
> *"We use Microsoft 365 and a few business tools."*

WHAT'S ACTUALLY HAPPENING

- Employees sign up for apps without IT approval
- Data gets stored across dozens of services
- Permissions and access controls are rarely reviewed

Even security leaders report that tool sprawl creates operational complexity and security gaps.

WHY IT MATTERS

- You lose visibility into where data lives
- You can't secure what you don't know about
- Former employees may still have access

HOW RHODIAN HELPS

We bring visibility and control back by:

- Centralizing identity and access management
- Enforcing least-privilege access policies

We help you reduce complexity and eliminate hidden risks.

RISK 04

Backups that don't actually protect your business

Almost every company says they have backups. Far fewer can actually recover from a disaster.

> WHAT MOST BUSINESSES THINK
>
> *"We have backups, so we're safe."*

WHAT'S ACTUALLY HAPPENING

- Backups aren't regularly **tested**
- Recovery times are too slow
- Backups can be deleted, encrypted by ransomware, or simply incomplete

WHY IT MATTERS

When something goes wrong, downtime can last days rather than hours, revenue stops immediately, and customer trust takes a hit. **Backup alone does not equal business continuity.**

HOW RHODIAN HELPS

We design backup and recovery that actually works:

- Immutable, ransomware-resistant backups
- Regular restore testing
- Defined recovery objectives (RTO/RPO)

The goal is simple: when something breaks, you recover fast.

RISK 05

Overconfidence: the risk that ties it all together

This is the most dangerous one — and the hardest to fix.

> WHAT MOST BUSINESSES THINK
>
> *"We're too small to be targeted."*

WHAT'S ACTUALLY HAPPENING

- Small and midsize businesses are increasingly targeted precisely because they're **easier to breach**
- Attacks are automated — no one is "choosing" you
- Most breaches exploit **basic gaps**, not advanced techniques

WHY IT MATTERS

Many businesses don't discover their vulnerabilities until after a ransomware attack, a data breach, or a business interruption. At that point, the damage is already done.

The bottom line

The biggest IT risks in 2026 aren't caused by sophisticated hackers breaking through advanced defenses. They're caused by gaps in identity security, a lack of visibility, misconfigured tools, and outdated assumptions.

What should you do next?

If you're not sure whether these risks exist in your environment, you're not alone. The good news: they're fixable — once you know where to look.

Start with a vulnerability assessment. A proper one will show you:

- Where your biggest vulnerabilities are
- How exposed your users and data really are
- What needs to be fixed first

Or maybe you just want a second opinion

Rhodian can help you identify gaps in:

- Security
- Backup and recovery
- User access
- Device management

No jargon. No pressure. Just a clear view of your risks.

FINAL THOUGHT

Most IT issues don't come from what you *know* is wrong. They come from what you don't realize is a risk yet.

RHODIAN

Written by Pascal Eggers — Rhodian Group