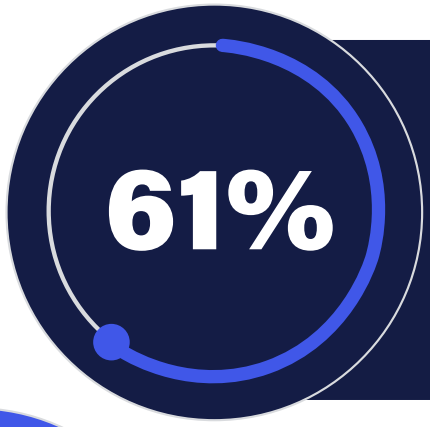
rightworks

GUIDE

# Essential steps to secure your small business

# **Cybersecurity:** Why it should be a priority for your small business




**61% of small businesses were victims of a cyberattack in the last year.**

**Source: BlackFog**




**The average cost of a data breach for small businesses rose 13% in 2023.**

**Source: IBM Security Cost of a Data Breach Report 2023**

In today's digital environment,  cybersecurity isn't just an investment—it's a necessity for small businesses. This guide will help you understand the risks and provide actionable steps you can take to protect your business.

## Get the facts: What you need to know about cybercrime

Small businesses are increasingly becoming targets for cybercriminals due to their sometimes-limited security resources. The statistics are alarming: **61% of small businesses experienced a cyberattack in the past year**, with 58% of victims facing business downtime and nearly 40% losing customer data. The financial impact is significant, with the average cost of a data breach rising 13% for small businesses in 2023. And the reputational damage can be even more costly.

# Understand the threat: The risks of inadequate cybersecurity

Cyberattacks can have devastating consequences for small businesses. Understanding these risks is the first stage in recognizing the importance of robust cybersecurity measures.

## Financial impact

- The average cost of breached records can quickly add up, potentially costing a small business thousands or even millions of dollars.
- With 57% of businesses **Increasing their prices** after a data breach, the potential for staying competitive is at risk.

## Customer trust

- The customer loss rate can be devastating, expecially for businesses in competitive markets or those relying on repeat customers.

## Business survival

- Cybercrime poses an existential threat to small businesses, leaving owners feeling uncertain about their business's survival after a cyberattack.

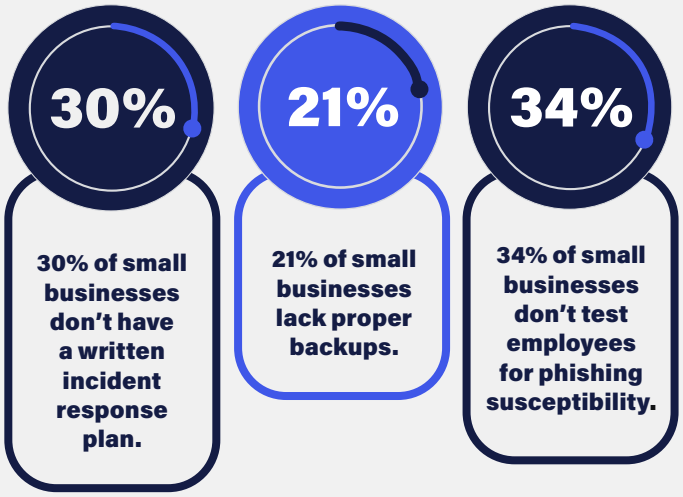








# Protect your business: 4 actionable steps to improve cybersecurity




**Source: CyberCatch Small and Medium-Sized Businesses Ransomware Survey**

To protect your business from cyberthreats, consider implementing the following four steps. These actions can help mitigate risks and enhance your overall security posture.

## 1. Develop a written incident response plan.

The Cybersecurity and Infrastructure Security Agency (CISA) recommends that small businesses have a **written incident response plan** to help them in their efforts to secure customer, employee and business data.

This plan helps businesses prepare for threats and outlines steps to take in case of a cyberattack, minimizing downtime, financial impact and recovery time.

Having this plan enhances customer trust, improves efficiency and ensures legal compliance.

## 2. Create adequate backups.

Granular backups protect data from ransomware attacks and ensure business continuity.

Businesses need backup redundancy and regular testing to protect against data loss and to verify that the backups are working properly.

Working with a managed security provider offers advantages to small businesses because they can handle server maintenance, application updates and data storage/backup.

## 3. Implement employee phishing tests.

Regular testing helps identify vulnerabilities and trains employees to recognize threats.

Training employees with real-life scenarios mitigates cybersecurity risks by addressing the increased threat faced by small businesses.

Phishing tests establish a measurable system to identify areas for improvement and allow businesses to focus and allocate resources on exposed issues.

## 4. Trust the experts.

Independently implementing and maintaining a comprehensive and robust security strategy can be complicated for small businesses, but cybersecurity experts can simplify the process.

Managed security providers provide round-the-clock threat monitoring that ensures businesses are protected 24/7.

These external solutions are not only easy to implement but they're also cost-effective, giving businesses peace of mind without breaking the bank.

# Choose the right cybersecurity partner:
# What you should look for

Selecting the right cybersecurity partner is critical for ensuring the complete protection of your business. You need comprehensive services that cover all aspects of cybersecurity, from technological solutions that secure your core business applications to employee training and ongoing support. A good partner will fill the security gaps and provide peace of mind, allowing you to focus on what matters most—running your business.

## When you partner with Rightworks for your cybersecurity needs, you get:

1. **Cloud-based application access**
   Allows employees to work securely from anywhere, enhancing flexibility.

2. **Server maintenance and updates**
   Ensures systems are always up to date and protected against the latest threats.

3. **Data storage and backup**
   Provides secure, redundant storage to prevent data loss.

4. **Enterprise-level data center security**
   Offers protection far beyond what most small businesses can implement on their own.

5. **Device security for remote work**
   Protects against threats regardless of where employees are working.

6. **Enhanced email protection**
   Safeguards against the most common type of cybercrime, which is crucial given that **90% of cyberattacks start with phishing emails**.

7. **Employee cybersecurity training**
   Addresses the human element, which is involved in **68% of data breaches.**

8. **Reliable support**
   Delivers award-winning 24/7 proactive support and guidance from a trusted, expert team.

## Focus on running your business and let the experts handle your cybersecurity needs.

## Protect your business today!

**866.691.4291**

rightworks

rightworks.com