EXECUTIVE REPORT

# 2026 Cybersecurity & Business Risk Report

## What Business Owners Need to Know

REDUCE RISK.
PROTECT
WHAT MATTERS.

STRENGTHEN
RESILIENCE.
DRIVE GROWTH.

EMPOWER
CONFIDENCE.
SECURE THE FUTURE.

Prepared by

Superior Technical Solutions

STS
SUPERIOR
TECHNICAL SOLUTIONS

# Executive Summary & 2026 Threat Landscape

Cybersecurity is now a business continuity issue—not just an IT issue.

Small businesses are more connected, more digital, and more targeted than ever before. As technology dependence grows and threats become more sophisticated, a single disruption can impact operations, reputation, and long-term profitability. Understanding the 2026 threat landscape is the first step toward building a stronger, more resilient business.

## What Changed in 2026

- AI-assisted phishing is more convincing
- Attackers exploit vulnerabilities faster
- Cloud and vendor dependencies create more third-party risk
- Operational disruption is often the greatest business impact

## Most Common Small-Business Risks

- Email compromise
- Ransomware
- Stolen credentials
- Shadow AI and unmanaged app use

### Key Takeaway

The goal is not to eliminate all risk. It is to reduce exposure, improve detection, and recover quickly when something goes wrong.

# Cybersecurity by the Numbers

A few figures show why cyber risk belongs on the leadership agenda.

**1,008,597**

internet-crime complaints reported to the FBI in 2025

**$20.9B**

in reported internet-crime losses during 2025

**$3.04B**

in reported business email compromise losses during 2025

**31%**

of organizational breaches analyzed began with vulnerability exploitation

**62%**

of breaches analyzed involved a non-malicious human element

**$4.99M**

global average cost of a data breach

## What these figures mean

For small businesses, operational downtime, recovery costs, and lost revenue can become severe even when losses are smaller than enterprise-scale breaches.

## Important to remember

Business disruption is often the biggest cost. Even a short outage can impact customers, cash flow, and long-term trust.

Sources: FBI IC3 2025 Annual Report; Verizon 2026 DBIR; IBM Cost of a Data Breach Report 2026.

# The Top Risks Facing Small Businesses

Most incidents begin with a manageable weakness — but the business impact can spread quickly.

## 1 Business email compromise and payment fraud

Fraudulent payment requests, changed bank details, payroll diversion, and executive impersonation can turn a believable message into a direct financial loss.

## 2 Ransomware and operational disruption

Attackers may encrypt systems, steal data, and interrupt scheduling, billing, communication, or service delivery.

## 3 Stolen passwords and account takeover


Reused passwords, phishing pages, and weak access controls can expose email, cloud files, payroll, or administrative systems.

## 4 Unpatched systems and aging technology

Unsupported systems and delayed security updates give attackers a predictable route into the network.

## 5 AI-related risks and shadow AI

Employees may place confidential information into unapproved AI tools or connect AI apps to business systems without oversight.

## 6 Vendor and supply-chain risk

A vendor, software provider, or cloud service can become the path into the business or a source of operational interruption.

Sources: FBI IC3 2025 Annual Report; Verizon 2026 DBIR; CISA small-business and ransomware guidance.

# How Cyber Incidents Affect the Business

The greatest cost is often the interruption — not the initial technical event.

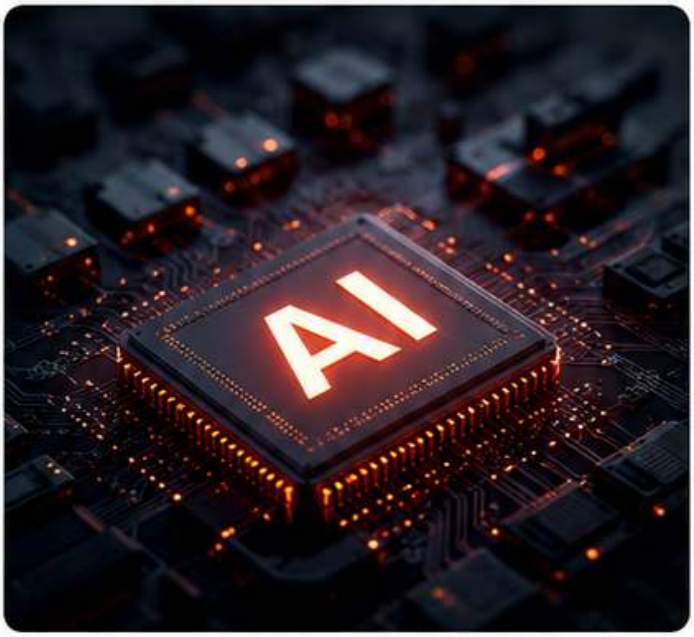

**The greatest cost of a cyber incident is often not the ransom or stolen data.**
**It is the interruption to the business.**

**How long could the organization continue serving customers if email, files, scheduling, billing, or a core business application became unavailable?**

Source: Context: CISA #StopRansomware Guide; IBM Cost of a Data Breach Report 2026.

# AI, Cloud Applications & Emerging Risk

AI tools and cloud platforms create real efficiencies for businesses, but unmanaged use introduces new exposure.




### AI-ENABLED ATTACKS ARE RISING

Attackers use AI to automate phishing, generate malware, and exploit vulnerabilities at scale—often faster than defenses can adapt.

### SHADOW AI CREATES BLIND SPOTS

Employees may use public AI tools and upload sensitive company data without IT knowledge—often without IT knowledge.

### DATA CAN BE EXPOSED

Information entered into public AI tools may be stored, used for training, or accessed by others.

### AI CONNECTED TO BUSINESS SYSTEMS

AI plugins and integrations can access email, files, calendars, and apps—expanding the potential impact of misuse or compromise.

### HUMAN REVIEW IS ESSENTIAL

AI-generated content can be inaccurate, incomplete, or biased. It should be reviewed before use.

### WHAT BUSINESSES SHOULD DO

- Establish an AI acceptable-use policy
- Define which tools are approved
- Prohibit input of sensitive or regulated data
- Review AI permissions and integrations
- Provide employee training and guidance

**45%**
of breaches involved cloud-based activity

**1 in 4**
malicious breaches studied were AI-enabled

# Cyber Resilience:
# Protect, Detect, Respond, Recover

Strong cybersecurity is more than prevention. Resilience means the business can withstand disruption and recover quickly.

## PROTECT

Reduce the likelihood of an incident by implementing strong security controls.

- MFA & access controls
- Patch management
- Email security
- Endpoint protection
- Employee training

## DETECT

Monitor your systems and environments to identify threats early.

- Continuous monitoring
- Threat detection
- Log analysis
- Vulnerability alerts
- User behavior review

## RESPOND

Act quickly and effectively to contain threats and minimize business impact.

- Incident response plan
- Clear responsibilities
- Communication plan
- Containment steps
- Third-party coordination

## RECOVER

Restore critical operations and return to normal operations as quickly as possible.

- Tested backups
- Recovery priorities
- Business continuity
- Lessons learned
- Continuous improvement

Resilience is not built in a day—it is built through consistent planning, testing, and improvement.

# 2026 Priorities for Small Businesses

Focus on what matters most. These six priorities help reduce risk, strengthen resilience, and protect what the business has built.

## 1 KNOW WHAT YOU DEPEND ON

Maintain an accurate inventory of devices, software, cloud services, and data. The business cannot protect what it cannot see.

## 2 PROTECT ACCOUNTS

Require MFA, use a password manager, and limit access to only what is needed.

## 3 PATCH AND MODERNIZE

Keep systems and applications up to date. Replace unsupported or end-of-life technology before it becomes a liability.

## 4 STRENGTHEN FINANCIAL SAFEGUARDS

Verify payment requests, implement approval processes, and protect against business email compromise.

## 5 TEST BACKUP AND RECOVERY

Back up critical data, test restores regularly, and ensure the business can recover quickly.

## 6 PREPARE PEOPLE AND PLANS

Train employees, run phishing simulations, and keep an incident-response plan ready.

Cyber resilience means making the business **harder to disrupt—and easier to recover.**

# Questions Every Leader Should Ask

Use these questions in leadership meetings or annual planning sessions to evaluate the organization's cybersecurity posture.

## TECHNOLOGY

- [ ] Which systems are critical to daily operations?
- [ ] Are any systems unsupported or approaching end of life?
- [ ] How quickly are critical vulnerabilities addressed?
- [ ] Are all devices monitored, managed, and protected?

## ACCOUNTS & ACCESS

- [ ] Is MFA enabled on all critical systems?
- [ ] Are administrative accounts separated from daily use?
- [ ] How often do we review user access?
- [ ] How quickly is access removed when an employee leaves?

## RECOVERY & RESPONSE

- [ ] What data and systems are backed up?
- [ ] When was our last successful restoration test?
- [ ] How long would it take to recover critical operations?
- [ ] Do we have an incident-response plan?

## PEOPLE & VENDORS

- [ ] How are employees trained on security?
- [ ] Do we test employees with phishing simulations?
- [ ] Which vendors have access to our data or network?
- [ ] What AI tools are employees using, and are they approved?

A useful answer should identify a **named owner**, a **documented process**, **evidence** that the control is working, and a **date** for the next review.

# From Cybersecurity to Business Resilience

The strongest programs are built through consistent decisions and continuous improvement.

No organization can guarantee that it will never experience a cyber incident. Even well-protected businesses can be affected by newly discovered vulnerabilities, vendor failures, employee mistakes, or sophisticated attacks.

**The practical objective for 2026 is straightforward: make the business harder to compromise, limit the damage an attacker can cause, and be prepared to restore operations when something goes wrong.**

**Recommended next step:**

- Review your cybersecurity posture
- Evaluate backup and recovery readiness
- Assess technology lifecycle and system health
- Review vendor access and third-party risk
- Evaluate AI usage and data protections
- Test incident response preparedness

**Not sure how your business would answer the questions in this report?**

STS offers a complimentary 10-minute **Cyber Risk Conversation** to help business owners determine whether a deeper review would be worthwhile.

**435-313-8132**

## Primary sources

- FBI Internet Crime Complaint Center, 2025 IC3 Annual Report.
- Verizon, 2026 Data Breach Investigations Report and May 19, 2026 findings summary.
- IBM, Cost of a Data Breach Report 2026 and July 29, 2026 findings summary.
- CISA, Cyber Guidance for Small Businesses and #StopRansomware Guide.
- NIST, Cybersecurity Framework 2.0 and small-business implementation guidance.

**Educational notice:** This report provides general educational information and is not legal, regulatory, insurance, or compliance advice.

## Recommended next step:

Review your cybersecurity posture

Evaluate backup and recovery readiness

Assess technology lifecycle and system health

Review vendor access and third-party risk


Evaluate AI usage and data protections

Test incident response preparedness

## Not sure how your business would answer the questions in this report?

STS offers a complimentary 10-minute **Cyber Risk Conversation** to help business owners determine whether a deeper review would be worthwhile.

**435-313-8132**

### Superior Technical Solutions

Your Dedicated IT Arm - helping businesses reduce risk, strengthen resilience, and plan technology with confidence.