Shumaker

OCTOBER 9, 2025 | PUBLICATION

"Cybersecurity Tips for Businesses"

Why It Matters

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

- Reputation at Risk: Customers lose trust quickly after a breach.
- Legal & Financial Consequences: Fines, lawsuits, and regulatory penalties add up fast.
- Operational Disruption: Downtime and recovery can cost more than prevention.

Proactive Preparation

Know Your Data

- Map where sensitive information (PII, PHI, financial data) is stored and shared.
- Limit access to "need-to-know."

Strengthen Defenses

- Use multi-factor authentication (MFA).
- Patch and update systems regularly.
- Encrypt sensitive data at rest and in transit.

Vendor Management

- Review contracts for cybersecurity and data handling obligations.
- Require business associate agreements (BAAs) or data processing agreements (DPAs).

Incident Response Readiness

Create a Breach Response Plan

- Define roles: legal, IT, HR, PR, leadership.
- Draft internal and external communication templates.

Test the Plan

- Run tabletop exercises at least annually.
- Simulate common scenarios (phishing, ransomware, lost laptop).

Legal & Regulatory Awareness

- Stay current on state, federal, and industry-specific breach notification laws.
- Know when you must notify regulators, customers, or partners.

Ongoing Security Practices

Train Employees

- Phishing awareness, safe data handling, and incident reporting.
- Make training continuous, not once-a-year.

Minimize Data

- Collect only what you need, keep only as long as required.
- Delete outdated or unnecessary information securely.

Communicate Clearly

- Transparent privacy notices and opt-out options build trust.
- Provide clear "Do Not Sell/Share" links where required.

Quick Wins for Businesses

1. Enable MFA for all accounts.
2. Review vendor contracts for data protection.
3. Update your incident response plan this quarter.
4. Train staff on phishing every 90 days.
5. Encrypt sensitive files before sharing.

A breach isn't if—it's when. Businesses that prepare in advance reduce financial damage, regulatory exposure, and loss of trust.

Shumaker