BRIGHTADVISOR®

Cybersecurity Assessment Guide

Evaluate and Strengthen Your Organization's Security Posture

4450 S. Rural Rd, Suite B-132, Tempe, AZ 85282 | (602) 497-0277 | brightadvisor.com

Why Regular Security Assessment Matters

Cybersecurity is no longer an IT issue; it is a business survival issue. The threat landscape evolves daily, with attackers increasingly targeting small and mid-sized businesses that lack the sophisticated defenses of large enterprises. A regular, structured security assessment is your first line of defense, identifying vulnerabilities before they are exploited.

> 43% of all cyberattacks target small businesses, yet only 14% of small businesses rate their ability to mitigate cyber risks as highly effective.

> The average cost of a data breach reached $4.88 million in 2024 (IBM Cost of a Data Breach Report). For small businesses, the impact is proportionally devastating.

> 60% of small businesses that suffer a significant cyberattack close their doors within six months. The damage extends beyond financial loss to reputation, customer trust, and regulatory penalties.

Threat Landscape Overview

Understanding the most common attack vectors helps prioritize your defenses. Here are the threats most likely to impact your organization.

Threat	Prevalence	Primary Target	Typical Impact
Phishing / Social Engineering	Very High	Email users	Credential theft, ransomware delivery
Ransomware	High	File servers, endpoints	Data encryption, business disruption
Business Email Compromise	High	Finance, executives	Wire fraud, data exposure
Insider Threats	Medium	Sensitive data access	Data theft, sabotage
Supply Chain Attacks	Growing	Vendor integrations	Backdoor access, malware
Unpatched Vulnerabilities	Very High	Servers, software	

			Remote exploitation, data breach

Security Assessment Checklist

Network Security

Control	Status	Priority	Notes
Firewall properly configured with documented rules		Critical	Review rules quarterly
Network segmented (guest, corporate, server, IoT)		High	Isolate sensitive systems
Intrusion detection/prevention system (IDS/IPS) deployed		High	Monitor and alert on anomalies
VPN required for all remote access		Critical	No split tunneling
Wireless security using WPA3 with unique SSID/passwords		High	Disable WPS, hide SSID optional
DNS filtering enabled to block malicious domains		Medium	Layer of defense against phishing

Identity & Access Management

Control	Status	Priority	Notes
Multi-factor authentication on all accounts		Critical	Prioritize email, VPN, admin accounts
Password policy enforced (12+ chars, complexity)		Critical	Consider passwordless options
Least-privilege access principle applied		High	Users get minimum required access
		High	

For educational purposes only. This guide does not constitute financial, tax, or legal advice. Consult a qualified financial advisor, tax professional, or attorney before making any financial decisions. BrightWealth® and BrightAdvisor® are registered trademarks.

Access reviews conducted quarterly			Remove terminated/changed-role access
Single sign-on (SSO) implemented		Medium	Reduces password fatigue and risk
Privileged accounts have separate credentials		Critical	Admin accounts not used for daily work

Endpoint Protection

Control	Status	Priority	Notes
EDR/antivirus on all endpoints with auto-updates		Critical	Next-gen EDR preferred over legacy AV
Patch management: OS and apps updated within 30 days		Critical	Critical patches within 72 hours
Full-disk encryption on all laptops and desktops		High	BitLocker (Win) or FileVault (Mac)
Mobile device management (MDM) for company devices		High	Remote wipe capability required
USB and removable media policy enforced		Medium	Block or monitor USB usage

Email Security

Control	Status	Priority	Notes
Advanced spam/phishing filtering enabled		Critical	AI-based filtering recommended
Phishing simulation and training program active		High	Monthly simulations, ongoing training
DMARC, DKIM, and SPF records properly configured		High	Prevents email spoofing of your domain
Email encryption available for sensitive communications		Medium	TLS enforced, S/MIME or equivalent
		Medium	

For educational purposes only. This guide does not constitute financial, tax, or legal advice. Consult a qualified financial advisor, tax professional, or attorney before making any financial decisions. BrightWealth® and BrightAdvisor® are registered trademarks.

Data loss prevention (DLP) policies active			Detect sensitive data in outbound email

Data Protection

Control	Status	Priority	Notes
3-2-1 backup strategy: 3 copies, 2 media types, 1 offsite		Critical	Test restores monthly
Encryption at rest for sensitive data stores		High	Database, file server, cloud storage
Encryption in transit (TLS 1.2+ enforced)		High	All web, email, and API traffic
Data classification policy documented and enforced		Medium	Public, internal, confidential, restricted
Retention and disposal policies defined		Medium	Secure disposal of media and data

Compliance & Governance

Framework	Applicable?	Current Status	Next Audit Date
HIPAA (healthcare data)			
PCI-DSS (payment card data)			
SOC 2 (service organizations)			
CMMC (defense contractors)			
State privacy laws (CCPA, etc.)			
Cyber insurance requirements			

For educational purposes only. This guide does not constitute financial, tax, or legal advice. Consult a qualified financial advisor, tax professional, or attorney before making any financial decisions. BrightWealth® and BrightAdvisor® are registered trademarks.

Compliance is not security, and security is not compliance. Meeting a regulatory checklist does not mean you are safe. Use compliance as a baseline, then build additional controls based on your specific risk profile.

Risk Rating Matrix

After completing the assessment, assign a risk rating to each domain. Use the matrix below to categorize findings and prioritize your remediation efforts.

Rating	Description	Remediation Timeline	Recommended Action
Critical	Actively exploitable vulnerability or missing fundamental control	Within 72 hours	Immediate remediation; escalate to leadership; consider incident response retainer
High	Significant gap that could be exploited with moderate effort	Within 30 days	Prioritize in next sprint; assign dedicated owner; track weekly
Medium	Control exists but is incomplete, outdated, or inconsistently applied	Within 90 days	Include in quarterly security improvement plan; verify at next assessment
Low	Minor improvement opportunity; defense-in-depth enhancement	Within 180 days	Add to backlog; address as resources allow; document for future reference

Scoring Your Assessment

Count the number of controls in each status category across all domains. A healthy security posture means zero critical findings, fewer than 3 high findings, and a clear plan to address all medium items within the quarter.

Status	Meaning	Count
Implemented	Control fully in place and verified	___
Partial	Control exists but gaps remain	___
Not Implemented	Control missing or non-functional	___
Not Applicable		___

For educational purposes only. This guide does not constitute financial, tax, or legal advice. Consult a qualified financial advisor, tax professional, or attorney before making any financial decisions. BrightWealth® and BrightAdvisor® are registered trademarks.

	Control does not apply to this environment

90-Day Security Improvement Plan

Use this phased approach to address your assessment findings systematically. Focus on the highest-impact items first, building momentum before tackling longer-term improvements.

Month 1: Foundation (Critical & Quick Wins)

- Enable MFA on all email, VPN, and admin accounts immediately
- Verify backup integrity with a test restore of critical systems
- Deploy or update endpoint protection (EDR) across all devices
- Patch all critical and high-severity vulnerabilities on servers and endpoints
- Conduct an emergency access review: disable dormant accounts and revoke excess privileges
- Review firewall rules and close unnecessary open ports
- Begin phishing awareness training for all employees

Month 2: Hardening (High-Priority Controls)

- Implement network segmentation for sensitive systems and guest WiFi
- Configure DMARC, DKIM, and SPF for all company email domains
- Deploy full-disk encryption on all laptops and workstations
- Establish a formal patch management policy with defined SLAs
- Document and test your incident response plan with a tabletop exercise
- Implement data loss prevention (DLP) policies for email and file sharing
- Enroll all company mobile devices in MDM with remote wipe capability

Month 3: Maturation (Medium-Priority & Governance)

- Finalize data classification policy and train employees on handling procedures
- Implement SSO for major business applications to reduce credential sprawl

- Establish quarterly access review process with documented sign-off
- Review and update cyber insurance policy based on assessment findings
- Create security awareness training calendar for the next 12 months
- Document all policies, procedures, and configurations for audit readiness
- Schedule next full security assessment for 6 months from today

> BrightWealth® cybersecurity services include comprehensive assessments, remediation planning, managed security monitoring, and ongoing compliance support. Our team helps businesses achieve enterprise-grade security without enterprise-grade complexity. Contact us for a complimentary security posture review.

For educational purposes only. This guide does not constitute financial, tax, or legal advice. Consult a qualified financial advisor, tax professional, or attorney before making any financial decisions. BrightWealth® and BrightAdvisor® are registered trademarks.