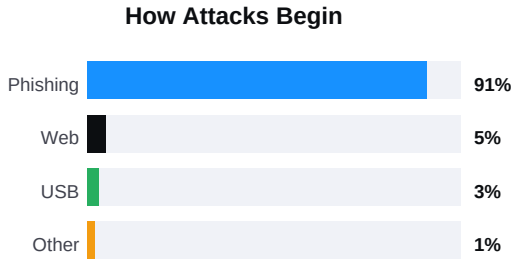
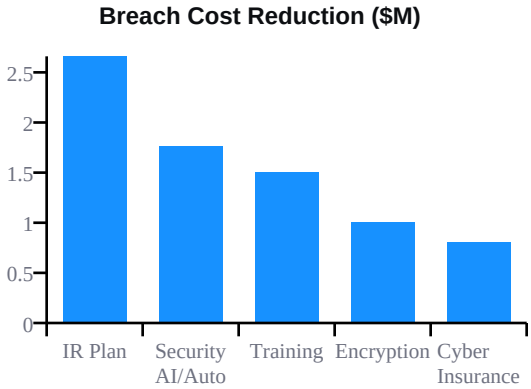
The 2026 Cybersecurity Playbook for Growing Businesses

A complete framework for protecting your business, clients, and reputation.

$4.88M	204	91%	43%
Avg breach cost	Days to detect	Start with phishing	SMBs lack a plan

Cybersecurity is a business risk that affects revenue, reputation, client trust, and regulatory standing. The companies that thrive are not the ones with the biggest budgets — they are the ones with the right framework, the right habits, and a security-first culture that starts at the top.





1. Asset Inventory & Data Classification

- Complete inventory of every device, cloud service, SaaS application, and user account. Classify data: Public, Internal, Confidential, Restricted. Identify crown jewels — data and systems that would cause the most damage if compromised
- Document all third-party vendors who access your systems or data. Maintain as a living document updated quarterly. A one-time inventory that sits in a folder is not a security control

2. Identity & Access Management

- MFA on every account without exception — blocks 99.9% of credential attacks. Conditional access policies evaluating risk signals. Least privilege: minimum access needed for each role, reviewed quarterly
- Privileged access management for admin accounts. SSO reducing password fatigue. Monitor for impossible travel alerts. Deploy business-grade password manager. Plan for passwordless authentication

3. Endpoint Protection

• Enterprise EDR on every device — traditional antivirus is not sufficient. Automatic patching within 48 hours of critical releases. Full-disk encryption on every laptop and workstation

• Application control on critical systems. Centralized device management with real-time compliance visibility. Include personal devices in security strategy if they access company data

4. Email Security

• Advanced threat protection with sandbox detonation. AI-powered phishing detection. DMARC/SPF/DKIM domain authentication. Data loss prevention on outbound email

• Monthly phishing simulations with targeted training. URL rewriting checking links at click time. Email archiving for compliance retention requirements

5. Network Security

• Segment guest WiFi, employee devices, servers, IoT, and cameras on separate network segments. Next-gen firewall with application-level inspection. DNS-layer security blocking malicious domains

• VPN or ZTNA for all remote workers. Monitor east-west traffic inside your network, not just internet traffic. Wireless security assessments to identify rogue access points

6. Backup & Disaster Recovery

• Follow 3-2-1-1-0: three copies, two media types, one offsite, one immutable, zero errors. Back up critical servers every 15-60 minutes. Test restores monthly with documented results

• Define RTO and RPO for every critical system. Store immutable backups in separate cloud account with different credentials. Annual full-scale DR drill

7. Security Awareness

• Training for all employees on hire and annually. Monthly phishing simulations tracking improvement. Train on social engineering: pretexting, baiting, tailgating

• Establish culture where reporting is encouraged and rewarded. Include leadership in training — executives are frequently targeted. Communicate about real-world incidents as learning opportunities

8. Compliance & Governance

• Identify applicable frameworks: HIPAA, PCI DSS, SOC 2, NIST, state privacy laws. Map controls to requirements, identify gaps, create prioritized remediation plan

• Written policies reviewed annually. Audit-ready documentation at all times — produce evidence within 24 hours if a regulator asks. Build compliance into daily operations through automated controls

9. Measuring & Improving

- Track Mean Time to Detect (target <24 hours vs 204 industry avg) and Mean Time to Respond. Monitor phishing click rates (target <5%) and patch compliance (target 95% within 14 days)
- Annual penetration testing by qualified third party. Benchmark maturity against frameworks. Report security metrics to leadership quarterly. Review all incidents monthly for trends

Ready to Put This Playbook Into Action?

Schedule a complimentary strategy session. We will assess your security posture and build a prioritized roadmap for your business.

elevatesolutions.io | (888) 901-9686

Elevate Solutions implements every control in this playbook for our managed IT clients. Our security stack covers all nine domains — from asset inventory and identity management through backup verification and compliance reporting. We do not sell individual point solutions; we deliver a complete, integrated security program managed by a dedicated team that knows your business.

Our clients across healthcare, legal, financial services, and professional services trust us to protect their most sensitive data, maintain compliance with industry regulations, and ensure business continuity when threats materialize. We provide 24/7 monitoring, monthly security reporting, quarterly business reviews, and a dedicated account manager who understands your environment and business objectives.

The organizations that avoid catastrophic security incidents are not the lucky ones — they are the prepared ones. They implemented this playbook before the attack arrived. When it did arrive, they detected it in hours instead of months, contained it before it spread, and recovered from tested backups within their defined recovery objectives. That preparation is what separates a minor disruption from a business-ending event.

Every control in this playbook is a layer in your defense. No single layer is sufficient. Firewalls fail. Phishing gets through. Employees click links. Backups are the last line. The businesses that survive are the ones with enough layers that when one fails — and one always will — the next layer catches the threat before it becomes a catastrophe. That is what defense in depth means in practice, and it is exactly what we build for every client. Contact Elevate Solutions at (888) 901-9686 or visit elevatesolutions.io to schedule your security assessment.