Phenicie Cybersecurity Strategy 2025

Practical protection for Polson & Lake County small businesses

Phenicie Business Management (PBM) — Managed IT & Security

We keep local businesses running without tech headaches — with a security-first approach grounded in prevention, detection, and fast response.

Text SECURE to (406) 382-9207 or visit phenicie.com/cyber-security-strategy

Executive Summary

Why this matters

Cyberattacks against small businesses are rising. Email-borne threats, weak passwords, outdated devices, and missing backups are the usual root causes. PBM’s strategy focuses on simple, enforceable controls that protect owners’ time and reduce downtime.

Our approach

- Prevent: Harden email, endpoints, and identities; secure backups; patch routinely.
- Detect: Monitor alerts, triage noise, escalate only what matters.
- Respond: Clear runbook, documented roles, tested backups, rapid comms.

What you get

- A Security Baseline (quick health check, 10 key controls)
- Ongoing managed protection & monitoring
- Incident response support with real-world SLAs

Next step

Text SECURE to (406) 382-9207 for the checklist and baseline.

Threat Model for Local SMBs

Top risks we see in Polson & Lake County

- Business Email Compromise (invoice/payment fraud, phishing, MFA fatigue)
- Endpoint Malware/Ransomware from unpatched systems or unsafe downloads
- Account Takeover due to reused/weak passwords and no MFA
- Data Loss from single-device storage or untested backups
- Vendor/Website Exposure (DNS, SPF/DKIM/DMARC misconfig, weak plugins)

Control philosophy

- Start with the first 10 controls (page 6).
- Document owners and SLAs.
- Measure monthly; improve quarterly.

Controls: Prevent • Detect • Respond

Prevent

- Email security: SPF/DKIM/DMARC, impersonation protection, phishing training
- Identity & access: MFA everywhere, password manager, conditional access
- Endpoint: EDR/AV, disk encryption, screensaver lock, USB control
- Patch & config: OS/3rd-party updates, least privilege, baseline hardening
- Backup: 3-2-1 backups with offsite copy; quarterly restore tests

Detect

- Alerting from EDR, email gateway, backups, and cloud identity
- Daily triage with rules to suppress noise
- Weekly summary to owners; monthly posture report

Respond

- Incident runbook (who does what, when)
- Isolation & containment steps for devices/accounts
- Communication templates (staff, clients, vendors)
- Forensics & evidence capture; post-incident review

Incident Response Snapshot

Severities & first moves

- Critical (active ransomware or takeover): isolate hosts, revoke sessions, disable accounts, trigger restore
- High (confirmed malware/phish landing): isolate device, reset credentials, scan tenants, notify affected users
- Medium (suspicious but unconfirmed): monitor closely, enable extra logging, user coaching

Backup & restore

- Offsite copy verified
- Quarterly restore test documented
- RTO/RPO targets agreed with owner

Documentation

- Ticket IDs, timeline, actions taken, artifacts collected
- Lessons learned, control updates, owner sign-off

Contact PBM

Text SECURE to (406) 382-9207 for help or email brady@phenicie.com

Security Baseline Checklist (10 Controls) & Next Steps

10 controls to reach baseline

- MFA on Microsoft/Google + key SaaS
- Password manager for staff
- SPF/DKIM/DMARC enforced
- Phishing training + quarterly simulations
- EDR/AV on all devices (with alerts)
- OS & app patching within 14 days (critical within 7)
- Disk encryption (BitLocker/FileVault)
- Role-based access + offboarding checklist
- 3-2-1 backups + quarterly restore test
- Device inventory + lost/stolen response

Ready to start?

Get the full checklist and baseline: phenicie.com/cyber-security-strategy
Or text “SECURE” to (406) 382-9207 and we’ll send the link.