CIPHEREX
SECURE INTERNETWORKING SOLUTIONS

Security Framework

Tier 1 — Stop the breach (critical, do first)

Phishing-resistant MFA

FIDO2 / passkeys for M365 and all SaaS.
Disable SMS/voice OTP for admin accounts.
Conditional Access to enforce everywhere.

MDR / EDR on every endpoint

Managed detection + response, not just AV.
24×7 SOC coverage (e.g. ArcticWolf, SentinelOne).
Isolate + respond in minutes, not days.

Email security (layered)

Defender P1 + advanced layer (Avanan/Proofpoint).
Block BEC, spear-phishing, impersonation.
DMARC enforcement + anti-spoofing.

Automated patch management

OS + 3rd-party apps patched within 14 days.
RMM-enforced (NinjaOne, Intune, etc.).
Critical CVEs patched within 72 hours.

Tier 2 — Contain the damage (important, do next)

Immutable, tested backups

3-2-1-1: 3 copies, 2 media, 1 offsite, 1 immutable.
Air-gapped or WORM cloud (Azure immutable vault).
Restore tested quarterly — not just assumed.

Least-privilege + PAM

No standing admin rights — use PIM/JIT access.
Separate admin accounts from daily-use accounts.
Privileged Access Workstations for IT admins.

Password manager (company-wide)

Every credential in a vault — no shared passwords.
SSO-integrated (e.g. Keeper, 1Password Business).
MFA required to access vault itself.

Security awareness training

Monthly simulated phishing (KnowBe4, Proofpoint).
Onboarding training + annual compliance module.
Track click rates; remediate repeat clickers.

Tier 3 — Harden and govern (build over 6–12 months)

DNS filtering + web proxy

Block C2 callbacks, malware domains, phishing URLs.
Works even when EDR is bypassed on endpoint.
Cisco Umbrella, Cloudflare Gateway, DNSFilter.

Vulnerability scanning

Quarterly internal + external scans (Tenable, Rapid7).
Prioritize by CVSS + exposure (internet-facing first).
Remediation SLAs tied to severity.

Incident response plan

Written runbook: who calls whom, in what order.
Tabletop exercise at least once a year.
Cyber insurance aligned to plan and coverage gaps.

Vendor / supply chain risk

Require SOC 2 or equivalent from key vendors.
Limit OAuth grants and third-party SaaS access.
Review and revoke inactive integrations quarterly.