FIREFLY
TELECOM CONSULTING

CYBERSECURITY **ESSENTIALS** For Your Business

A practical guide from your advocates at Firefly — approachable, jargon-light, and focused on outcomes.

Why Security Matters Right Now

Today's threats move fast and target the weakest link — often busy people and unmanaged devices. A single incident can trigger financial losses, reputational damage, and legal exposure. The good news: most risk can be reduced with a handful of proven basics.

What's changed: more remote/hybrid work, more cloud apps, and more connected devices at home and in the office — all creating new paths in for attackers.

What you can expect from Firefly: clear guidance, vendor-neutral recommendations, and a plan matched to your budget and risk.

Four common myths (and what's true)

- **"We're too small to be a target."** In reality, smaller organizations are frequently targeted because defenses are inconsistent. Basic protections go a long way.
- **"Compliance means we're safe."** Compliance is a minimum bar; attackers evolve faster than checklists. Think of compliance as a milestone, not the finish line.
- **"Cyber insurance covers it."** Insurance helps after an incident. It doesn't prevent downtime, data loss, or reputational harm — and it often excludes ransomware without strict controls in place.
- **"We'll handle it when it happens."** Response is easier and cheaper when you've prepared: trained people, documented steps, and the right tools already deployed.

Bottom line: Prevention and preparedness beat reaction every time.

The 7 must-do basics

Use these as a punch-list to strengthen your foundation. Firefly can help you implement each one.

1. **Annual third-party security audit:** Get an objective view of gaps and prioritized fixes.
2. **Security awareness training & testing:** Teach people how to spot phishing, handle suspicious devices, and report issues. Reinforce with brief tests.
3. **Managed firewall security:** Keep patches current and monitor round-the-clock. Next-gen firewalls add intrusion prevention and safer web filtering.
4. **Email security & encryption:** Stop phishing and account-takeovers; protect sensitive messages in transit.

5. **Supported, up-to-date hardware & software:** Retire end-of-life gear that can't be patched.
6. **Protected access (MFA + VPN/ZTNA):** Require multi-factor authentication for all accounts and secure remote access to company resources.
7. **Endpoint detection & response (EDR):** Protect every device — laptops, desktops, tablets, and phones — with modern endpoint security and the ability to isolate or wipe lost/compromised gear.

Bonus for hybrid work: segment home networks so company traffic stays separate from IoT gadgets; use Mobile Device Management (MDM) for BYOD.

How Firefly helps

Advise — We assess your current posture, explain trade-offs in plain English, and map controls to your risks and budget.

Implement — We source and coordinate the right mix of best-in-class security tools and managed services (training, email security, firewalls, EDR, MDM, VPN/ZTNA, audits) — all through a single, streamlined experience.

Support — Ongoing monitoring, updates, and reviews so security keeps pace with your business, not just the threat landscape.

How Firefly Operationalizes This For You

We bring in proven, best-fit options across SIEM, EDR, email security, firewalls, and more, then manage the rollout with minimal disruption. You get one accountable partner and a clear security scorecard.

Your First 90 Days with Firefly

We align to the NIST lifecycle—so you're covered from prevention through recovery—without drowning your team in jargon.

Days 0–30 | Assess & Align

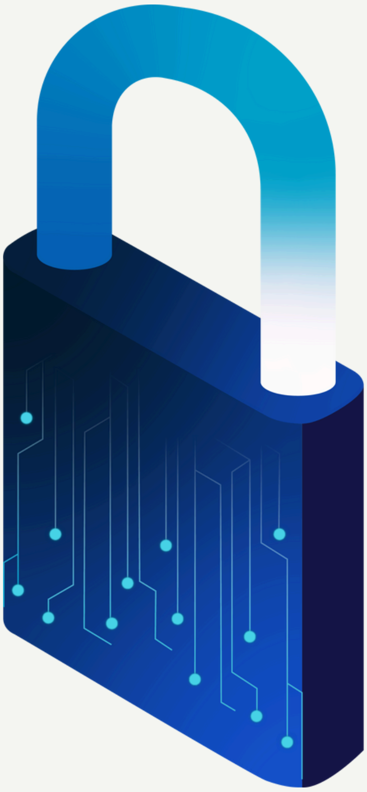
- Discovery workshop: goals, risks, regulatory needs, budget.
- Rapid assessment: email, endpoints, identity, cloud, network.
- 90-day action plan with quick wins (MFA everywhere; email filtering; high-risk patching) and a 12-month roadmap.

Days 31–60 | Protect & Detect

- Turn on MFA, EDR, and advanced email security.
- Tighten admin access; segment remote/home networks where needed.
- Enable logging + alerting (SIEM) for prioritized assets.

Days 61–90 | Respond & Recover, Govern

- Table-top exercise for your incident response plan.
- Test backup/restore and device wipe.



- Finalize metrics and cadence (monthly health checks, quarterly audits).

What you'll have:

- A right-sized security stack, tuned to your environment.
- Measurable risk reduction (fewer phishes clicked; blocked malware; faster patch SLAs).
- A partner who advocates for you, stays neutral on vendors, and keeps the path clear.

Let's Make This Easy:

Firefly delivers multi-layer protection—SIEM, endpoint security, ethical hacking/assessments, and more—through a single, accountable team. We design, implement, and support, so you can focus on your business. Ready to see gaps, fix them fast, and prove progress? Let's talk.

✉ info@fireflytele.com
🌐 fireflytele.com
📍 148 S Dowlen Rd, PMB 648, Beaumont, TX 77707