WHITE PAPER

The Complete IT Security Assessment Checklist

A practical, no-fluff security checklist for mid-size businesses with 30-200 employees. Covers the controls that actually matter.

eTop Technology | etoptechnology.com | 951-398-0021
611 W. Redlands Blvd., Suite G, Redlands, CA 92373

If you're running a business with 30 to 200 employees, you're big enough to be a real target but probably don't have a dedicated security team. This checklist is what we use at eTop Technology when we onboard clients and run annual security reviews. If you can't confidently say "yes" to an item, that's a gap worth investigating.

80%
of breaches involve compromised credentials

197
average days to detect a breach without monitoring

$4.88M
average cost of a data breach in 2024

1 Identity & Access Management

Access controls are the foundation. If the wrong people can get to the wrong data, nothing else matters.

- [ ] Multi-factor authentication (MFA) is enabled on all business email accounts
- [ ] MFA is enabled on all cloud applications (Microsoft 365, Google Workspace, CRM, accounting)
- [ ] VPN or remote access connections require MFA
- [ ] Administrative accounts use separate credentials from daily-use accounts
- [ ] Former employees are deprovisioned within 24 hours of departure
- [ ] User access is reviewed quarterly to ensure least-privilege principles
- [ ] Password policies require a minimum of 14 characters
- [ ] Shared accounts and generic logins have been eliminated
- [ ] Privileged access (admin rights) is limited to personnel who genuinely need it
- [ ] Single sign-on (SSO) is implemented where possible

WHY IT MATTERS

MFA alone blocks 99.9% of automated attacks. If you do nothing else on this list, get MFA deployed everywhere.

2 Endpoint Security

Every laptop, desktop, and mobile device is a potential entry point for attackers.

- [ ] All workstations and laptops run Endpoint Detection and Response (EDR), not just basic antivirus
- [ ] EDR is centrally managed with alerts going to a monitored dashboard
- [ ] Operating systems are patched within 14 days of critical security updates
- [ ] Third-party applications (browsers, PDF readers, Java) are patched regularly
- [ ] Full disk encryption is enabled on all laptops and mobile devices
- [ ] USB storage devices are restricted or disabled via policy
- [ ] Mobile device management (MDM) is in place for phones/tablets accessing company data
- [ ] Auto-lock is configured on all devices (5 minutes or less)
- [ ] Local admin rights are removed from standard user accounts

WHY IT MATTERS

EDR catches threats that antivirus misses by monitoring behavior patterns, not just known signatures. Encryption means a stolen laptop doesn't become a data breach.

3 Email Security

Email remains the #1 attack vector. If your email security is weak, the rest barely matters.

- [ ] Advanced threat protection scans attachments and links before delivery
- [ ] Impersonation protection is configured for executives and key personnel
- [ ] DMARC, DKIM, and SPF records are properly configured on your domain
- [ ] External email tagging (banner warnings) is enabled
- [ ] Automatic forwarding to external addresses is disabled or restricted
- [ ] Email retention and archiving policies are in place
- [ ] Users receive regular phishing simulation tests
- [ ] Phishing click rates are tracked; clickers receive additional training

WHY IT MATTERS

Over 90% of successful cyberattacks start with a phishing email. Your email configuration is the difference between an attack that gets caught and one that compromises your entire network.

4 Network Security

Your network connects everything. Without segmentation and monitoring, one compromised device can take down the whole operation.

- [ ] Firewall is enterprise-grade with active threat intelligence subscriptions
- [ ] Firewall rules are reviewed at least annually
- [ ] Network is segmented (servers, workstations, guest Wi-Fi, IoT on separate VLANs)
- [ ] Guest Wi-Fi is isolated from the corporate network
- [ ] DNS filtering blocks known malicious domains
- [ ] Remote access uses a modern VPN or zero-trust network access (ZTNA) solution
- [ ] Wireless networks use WPA3 or WPA2-Enterprise authentication
- [ ] Network traffic is monitored for anomalous behavior
- [ ] Intrusion detection or prevention system (IDS/IPS) is active

> **WHY IT MATTERS**
>
> Network segmentation prevents a ransomware infection on one workstation from spreading to your file server, backups, and every other system.

5 Data Backup & Recovery

Backups are your last line of defense against ransomware and data loss. But only if they actually work.

- [ ] All critical data is backed up at least daily
- [ ] Backups follow the 3-2-1 rule: 3 copies, 2 different media types, 1 offsite
- [ ] At least one backup copy is immutable (cannot be modified or deleted by ransomware)
- [ ] Backup integrity is verified automatically
- [ ] Full restore tests are performed at least quarterly
- [ ] Recovery time objectives (RTO) are defined and achievable
- [ ] Recovery point objectives (RPO) are defined and acceptable to the business
- [ ] Backup encryption is enabled for data at rest and in transit
- [ ] Backup access is restricted to authorized personnel only

WHY IT MATTERS

We've seen businesses discover during a crisis that their backups had been failing for weeks. Regular testing is the only way to know. Immutable backups save you when ransomware tries to encrypt your backup data too.

6 Security Awareness & Training

Your employees are the last line of defense, and often the first point of failure.

- [ ] All employees complete security awareness training during onboarding
- [ ] Ongoing training is conducted at least quarterly
- [ ] Training covers phishing, social engineering, password hygiene, and data handling
- [ ] Phishing simulations are conducted monthly
- [ ] Simulation results are tracked and used to target additional training
- [ ] Employees know how to report suspicious emails and activity
- [ ] There is a clear, no-blame policy for reporting potential security incidents

7 Policies & Documentation

If it's not written down, it doesn't exist from a compliance and audit perspective.

- [ ] Information security policy exists and is reviewed annually
- [ ] Acceptable use policy covers employee technology use
- [ ] Incident response plan is documented and rehearsed in the past year
- [ ] Business continuity and disaster recovery plans are documented
- [ ] Data classification policy defines handling of different data types
- [ ] Vendor management policy addresses third-party security requirements
- [ ] All policies are accessible to employees and acknowledged in writing

8 Compliance & Regulatory

Depending on your industry, you may have specific regulatory obligations.

- [ ] You've identified which regulations apply (FTC Safeguards, HIPAA, CMMC, PCI-DSS, state privacy laws)
- [ ] A designated individual is responsible for your information security program
- [ ] Risk assessments are conducted at least annually
- [ ] Penetration testing or vulnerability assessments are performed annually

- [ ] Cyber insurance policy is in place and covers ransomware, business interruption, and fines
- [ ] Insurance requirements are aligned with your actual security controls

How to Use This Checklist

Don't try to fix everything at once. Here's a practical approach:

1

Score Yourself

Go through each item. Mark yes, no, or partial.

2

Find Critical Gaps

MFA, EDR, and backups are the big three. Start there.

3

Build a 90-Day Plan

Pick the highest-impact items for the next quarter.

4

Get Outside Eyes

An external assessment catches what you missed.

Need Help Running This Assessment?

We do this for businesses across the Inland Empire every week. It takes a couple of hours and you'll walk away with a prioritized action plan. No cost, no obligation.

Schedule Your Free Assessment

etoptechnology.com | **951-398-0021**

611 W. Redlands Blvd., Suite G, Redlands, CA 92373