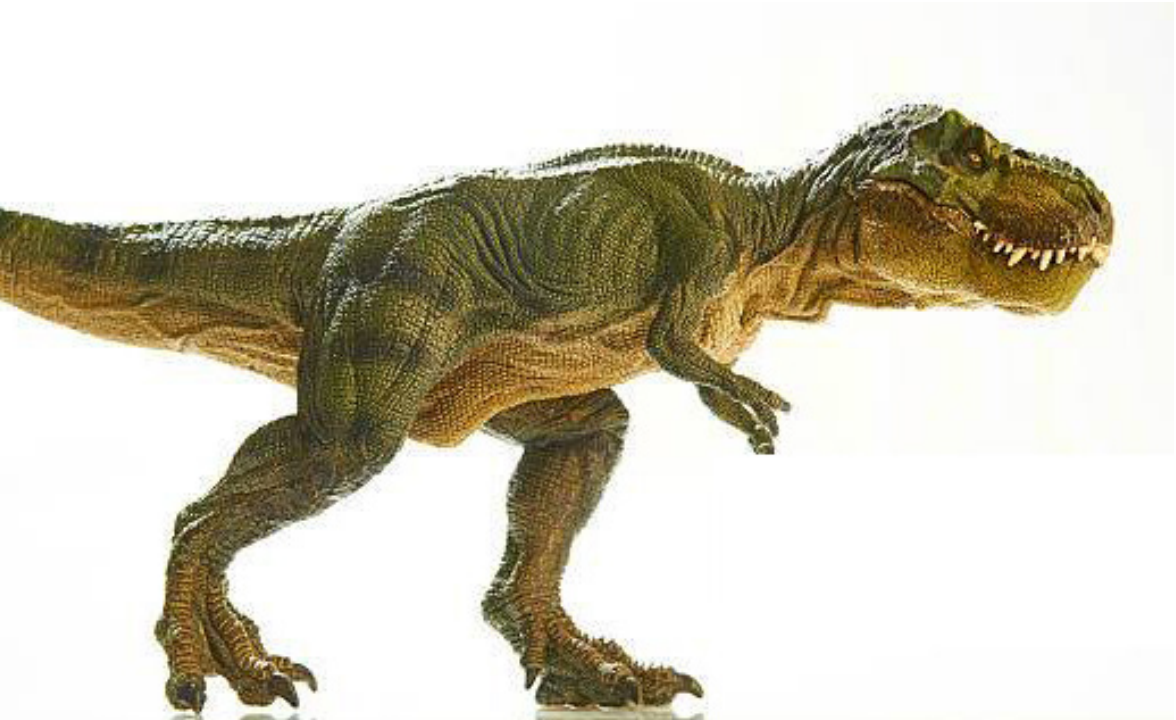
Ariel IT

*The cyber predators are out there. Don't let them attack **YOUR** business*

The Busy Business Leader's Ultimate Cybersecurity Checklist

Preparing for the worst is the best place to start.



The threats are coming. In fact, a recent analysis showed that Colorado is the U.S. state most at risk for cyber attack.

Cyber attacks cost U.S. businesses more than **a billion dollars a day.** Breaches result in downtime, lost revenue, employee stress, and reputational damage.

Sadly, it's safe to assume that your organization will be a periodic target of attack.

Proactive preparation is the only way to beat the cyber predators. Stronger protection and faster detection are the keys to success.

Using the checklist on page 4 , you can have confidence that you are actively reducing cyber risk for your organization. We know you find it useful, and we are always available to answer your cybersecurity questions.

Identity and access: who gets in… and who doesn't

Think of identity and access to your IT resources as the locks on your digital doors. Preventing account takeover avoids costly downtime and reputational damage. **Most cyber attacks begin with stolen logins**. That means that Multi-Factor Authentication (MFA), strong passwords, and role-based access stop criminals from logging in.

What To Do:

- Require MFA for all accounts, including administrators and service accounts.
- Create Admin accounts for administrative tasks, limiting user rights to only what's necessary.
- Use conditional access to block risky sign-ins and require healthy, compliant devices.
- Disable legacy protocols (POP/IMAP/basic auth) that bypass modern protections.
- Adopt a password manager and enforce unique passphrases.

Tools We Trust:

- Microsoft 365 Business Premium (identity, Conditional Access, Intune)
- Keeper MC Enterprise (password management)
- NordLayer Advanced (secure remote access)
- Huntress 24 x 7 detection and response)

Cybersecurity Checklist

You can use this Cybersecurity Checklist to verify that you and your people have all the necessary protections and controls in place to secure your IT environment.

Identity & Access

- ❏ MFA enabled for all users, admins, and service accounts
- ❏ Conditional access-compliant devices; risky sign-ins blocked
- ❏ Legacy protocols disabled (POP/IMAP/basic auth)
- ❏ Password manager deployed (Keeper Enterprise); unique passphrases
- ❏ No standing global admins; role-based access only

Endpoints (Windows/Mac)

- ❏ Layered Endpoint Protection (SentinelOne NGAV/EDR + Huntress MDR)
- ❏ Intune/Jamf baselines: BitLocker/FileVault, firewall on, app control
- ❏ Local admin removed, elevation workflow in place
- ❏ Monthly OS and third-party patching with SLA

Network

- ❏ Fortinet firewall IPS/IDS + application control enabled
- ❏ VLANs segment guest/IoT/sensitive systems; deny east-west by default
- ❏ Secure wi-fi (WPA3); per-SSID policies; 802.1X where feasible
- ❏ Firewall/IDS logs forwarded to SIEM

Email & Collaboration

- ❏ Ironscales deployed; users trained to report phish
- ❏ Microsoft Defender for Office 365 safe links/attachments on
- ❏ External sharing governance; DLP policies reviewed quarterly
- ❏ Quarterly phishing simulations; leadership report

Backup & Continuity

- ❏ Axcient/Axcient 365 configured; 3-2-1 rule met
- ❏ Backups immutable and encrypted
- ❏ Monthly restore test documented; RTO/RPO defined
- ❏ M365 (Exchange/SharePoint/OneDrive/Teams) backed up

Vulnerability & Configuration

- ❏ ConnectSecure scans weekly; remediation SLAs (Critical 7d / High 14d)
- ❏ Exceptions documented with compensating controls
- ❏ Baseline hardening applied (CIS-aligned)

Monitoring & Response

- ❏ Huntress SIEM/MDR active; alerting tested
- ❏ Incident response plan published; roles and playbooks defined
- ❏ Contact tree verified; annual tabletop exercise

Policies, People & Compliance

- ❏ AUP, Access control, incident response, backup policies signed
- ❏ Quarterly user training completed; metrics reported
- ❏ Compliance manager in place (NIST/CIS/CMMC mappings)
- ❏ Vendor risk reviews scheduled; insurance requirements met

Remote/Nonprofit/Mac

- ❏ NordLayer Advanced deployed; device-bound identity access
- ❏ Nonprofit Microsoft security licensing configured (Business Premium; Defender; Defender for Cloud Apps)
- ❏ Jamf baseline applied; Mac patching monitored

About Ariel IT Services

Colorado Front Range businesses and nonprofits turn to Ariel IT Services to optimize their IT investments and protect their data. Our decades of experience and proven expertise deliver the confidence that your computer systems will be up-to-date, running at peak efficiency, and protected from cybercriminals. We are also committed to helping you take care of your people by enabling them to stay productive without being preoccupied with security issues.

We provide fully managed IT services or can serve as your trusted co-managed IT partner. Our experts are adept at designing, deploying, and managing both on-premise and cloud-based systems, as well as creating hybrid models that combine the best of both worlds.

We are easy to work with, responsive to requests, and resourceful in solving problems. We take the time to understand your business, so we can recommend the best solutions. We are also invested in our community, supporting many good causes that make life better for all of us.

Our tagline says it all: ***Business Professionals—IT Experts****.*

Successful IT solutions come from partnerships built on trust. It's about people as much as technology, and we have the best of both.

Ariel IT

303.415.0266 • info@ArielITServices.com
1017 E. South Boulder Road, Suite B
Louisville, CO 80027
ArielITSevices.com