Mirazon
Providing Vision for Technology Solutions

Holiday IT Lockdown Checklist

Wrap Up the Year Without Wrapping Up a Cyber Incident

Before you hang up your stockings and shut your laptop for a long winter's nap, there are a few IT to-dos worth checking twice. Cyber Grinches love this time of year—but a quick holiday hardening sweep keeps your systems off their target list.

Here's your pre-holiday checklist to help you wrap things up the secure way.

#1 Verify Backups (Seriously... Check Them)

- [ ] Confirm the last successful backup dates for critical systems
- [ ] Run a quick restore test
- [ ] Ensure offsite/cloud backups are syncing as expected
- [ ] Confirm that retention policies are correct

Why it matters: Holiday ransomware attacks love a good untested backup.

#2 Patch the Big Stuff

- [ ] Apply any high/critical security patches you might have been pushing off
- [ ] Update firewall, VPN, and endpoint protection settings
- [ ] Review pending firmware updates for switches, firewalls, and servers

Why it matters: Attackers aim for unpatched systems over the holidays because no one is around to catch them.

Partnering with a Managed Service Provider (MSP), like Mirazon, helps to close these gaps.

#3 Shut Down or Tighten Unused Access

- [ ] Disable accounts for any recently offboarded employees
- [ ] Remove temporary access granted for projects that wrapped up
- [ ] Validate admin privileges (no “holiday surprises” in AD)
- [ ] Review shared accounts and ensure MFA is enabled

Why it matters: Dormant access is easy entry for bad actors.

#4 Double-Check MFA + VPN Settings

- [ ] Ensure MFA enforcement is active everywhere it should be
- [ ] Validate VPN configs and confirm logs are being monitored
- [ ] Make sure only approved devices can connect remotely

Why it matters: Remote access attempts and ransomware attacks spike by nearly 30% during the holiday season (November and December).

#5 Monitor Critical Alerts (Without Being Glued to Email)

- [ ] Verify alerting thresholds and escalation paths
- [ ] Confirm logs are flowing properly into your SIEM or monitoring tool
- [ ] Create automated dashboards or summary reports to quickly see issues at a glance

Why it matters: Fewer people are on call during the holidays, so smart alerting is critical. An MSP, like Mirazon, can help by monitoring alerts *for* you, fine-tuning thresholds, and ensuring you’re only notified when action is truly needed.

#6 Secure Holiday Hours for IT Staff

- [ ] Confirm who’s on call for emergencies
- [ ] Document where/how to contact vendors quickly
- [ ] Ensure leadership knows the escalation plan

Why it matters: Clarity prevents panic when something blips.

#7 Review Physical Security

- [ ] Verify server room access restrictions
- [ ] Ensure cameras and access control systems are logging properly
- [ ] Notify facilities of any planned closures

Why it matters: Offices empty out—attackers know it, too.

#8 Communicate "Safe Holiday Behavior" to Employees

- [ ] Warn them about common phishing attempts, like fake tracking emails and fraudulent sites
- [ ] Remind them to avoid using personal devices for work
- [ ] Encourage reporting suspicious activity and provide instructions on how to do it

Why it matters: Employee mistakes spike during gift-shopping season.

Pro tip: Send them our Holiday Cyber Survival Guide for more ways they can stay safe this holiday season.

By running through this checklist, you're giving your IT environment the gift of peace of mind. A few small actions now can prevent major headaches later, keep your systems humming, and make sure your team's holiday is spent celebrating—not troubleshooting.

Want a Complete Holiday IT Checkup? Your IT Elves Are Standing By!

We can run through this list (and the bigger behind-the-scenes version) for you—ensuring you're locked down and ready to enjoy the break without worrying about midnight alerts.

Mirazon®

Contact Us