Software Updates & Patch Management

Cyber Risk Mitigation

Many companies believe they are "up to date." Attackers know otherwise.

WHY THIS MATTERS TO YOUR BUSINESS

Many cyber insurance claims stem from unpatched systems. Once vulnerabilities are disclosed, attackers often exploit them within days. While servers are usually prioritized, employee devices are frequently overlooked, and delayed updates can create security gaps and potential coverage issues.

Over 50% of successful breaches involve unpatched or outdated software.

WHAT WE TYPICALLY SEE

- Systems are patched, but not consistently tracked
- Vendors release updates faster than IT teams can review them
- Remote devices fall outside normal update processes
- Organizations rely on manual updates instead of automated monitoring

IMPROVE PATCH DISCIPLINE

1. **Know what you actually have.**
   You cannot patch what you do not track. Maintain an accurate inventory of all devices and software.
2. **Automate wherever possible.**
   Automated patching reduces the lag time between vulnerability disclosure and remediation.
3. **Monitor vendor alerts.**
   Critical vulnerabilities often require immediate action before the next scheduled update cycle.

LP helps clients strengthen patch management.

Identify systems most likely to create exposure risk

Align patching practices with insurer security expectations

Integrate patch management into broader risk planning

Reduce the likelihood and cost of cyber incidents

Not sure whether your patch practices meet today's cyber insurance expectations?

LP can help you evaluate vulnerabilities and strengthen your cyber risk strategy.