Multi-Factor Authentication

Cyber Risk Mitigation

Cyber risks are no longer a technical issue—they're a business issue.

Multi-Factor Authentication is A Simple Step With Outsized Impact

Implementing MFA is a low-cost control that prevents the vast majority of credential-based cyber incidents. For most organizations, it's the single best first step toward reducing business interruption and financial loss.

What is MFA?

Multi-Factor Authentication (MFA) adds an extra verification step beyond your password—such as a text code, authentication app, biometric scan, or hardware token. Even if a password is stolen, MFA stops most unauthorized access attempts.

Compromised accounts carry risk and can have a high financial impact.

Prioritize MFA for:

- Email platforms
- Payroll and HR systems
- Banking and vendor payment portals
- Remote desktop and VPN access
- Cloud software tools containing client or employee data

How to Implement MFA

1. **Choose Strong MFA Methods.** Authentication apps, hardware tokens or keys and biometrics are superior to *SMS codes.*

2. **Roll Out MFA in Phases.** Start with admin accounts and financial systems and expand to all employees. Require MFA for any remote connection to the network.

3. **Train Your Workforce.** Explain why MFA matters and ensure employees know how to login and get support.

4. **Monitor & Enforce.** Require MFA during password resets, review accounts that have MFA disabled, and enforce through your identity provider.

Employee Security Training

Cyber Risk Mitigation

Cybersecurity is not just an IT responsibility.

Building a Security First Culture

Most cyber incidents do not begin with sophisticated hacking. They begin with human mistakes such as clicking on a malicious link or opening a harmful attachment.

Security awareness training helps ensure every employee:

- Understands today's most common cyber threats
- Knows how to recognize suspicious activity
- Follows company security & best practices

Employee Role in Cyber Security

Every employee plays a critical role in protecting their company, clients, and partners from cyber threats.

How to Prioritize Training:

- All employees - baseline training
- Additional training based on job function or access level should be incorporated
- Include regular freshers to address evolving threats
- Include realistic simulations and examples

Carrier insights / LP Offerings

- **Over 80% of cyber security incidents involve human error**
- **Phishing remains the #1 entry point for attackers**
- **Most breaches start with a single compromised user account**
- **Reach out to us today to learn more**

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.

Software Updates & Patch Management

Cyber Risk Mitigation

Software updates & security patches are two of the most important defenses organizations have against cyber attacks.

What patch management does

A structured patch management program helps organizations close security vulnerabilities before they can be exploited, reduce exposure to ransomware & malware, improve system stability & performance, maintain compliance with cybersecurity frameworks & insurance requirements, and protect sensitive client and financial information.

Software & Cyber Security Tips

- Critical software vulnerabilities are discovered every week
- Attackers often weaponize vulnerabilities within days of public disclosure
- Ransomware groups frequently target unpatched systems

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

Tips on How to Get Started with your risk mitigation playbook

- Maintain an Accurate Inventory
- Enable Automatic Updates Where Possible
- Monitor Vendor Security Alerts

Through cybersecurity advisory and risk management services, LP helps organizations:

- **Identify** systems requiring regular patching
- **Establish** update and vulnerability management processes
- **Integrate** patching with broader cybersecurity programs
- **Support** incident prevention and operational resilience

Proactive patch management is a key component of a strong cybersecurity posture.

Contact LP today to learn more about your company's specific vulnerabilities.

Enforce Strong Access Controls

Cyber Risk Mitigation

Sophisticated Hack or Wrong Person with Wrong Access?

Most cyber incidents don't start with a sophisticated hack. In fact, 81% start with compromised or misused privileged credentials.

Access control failures are a leading driver of cyber claims. When permissions are too broad or not regularly reviewed, a single compromised credential can expose critical systems, data, and operations. In many cases, the issue isn't lack of security tools—it's lack of discipline around who has access and why.

Least-Privilege Policy: Where Organizations Get this Wrong

- Employees retain access long after roles change
- Administrative privileges are granted "temporarily" but never removed
- Access reviews are informal or inconsistent

3 Ways to Strengthen Access Control

1. **Limit access by role—not convenience**
   Ensure employees only have access required for their current responsibilities
2. **Review access regularly**
   Quarterly reviews help catch unnecessary or outdated permissions
3. **Secure privileged accounts**
   Use MFA and tightly control administrative access

Insurers Look For

✓ Role-based access controls across systems

✓ Strong protections for administrative accounts

✓ Documented processes for access reviews

How LP Helps

✓ Identify access control gaps that could impact coverage.

✓ Align controls with evolving cyber insurance requirements

✓ Strengthen governance around privileged access.

ITIAL DRAFT

Back Up Critical Data & Test Recovery Plans

Cyber Risk Mitigation

Recovery testing ensures systems, data, personnel, and procedures are prepared before an incident occurs.

Backups are only valuable if it can be successfully restored

Data is one of the most valuable assets organizations possess. Backups and recovery planning are critical to every organization.

Many organizations assume backups are functioning correctly without ever validating recovery.

Common issues discovered during testing include:

- Corrupted backup files
- Incomplete backups
- Outdated recovery procedures
- Staff uncertainty during restoration

Different systems require different backup schedules:

- Daily backups for critical systems
- Frequent backups for financial or operational data
- Long-term retention for regulatory or business needs

Systems to Routinely Test

- File restoration
- System recovery
- Application recovery
- Disaster recovery scenarios

Carrier insights / LP Offerings

- **Identify critical data systems.** Which systems and data are essential to operations
- **Follow the 3-2-1 Backup Principle** Three copies of important data, two different storage types, and one copy stored offsite or offline
- **Protect backup systems.** Restrict administrative access, use MFA for backup platforms, continually monitor for suspicious activity.
- **Backups alone are not enough**

Back Up Critical Data & Test Recovery Plans

Cyber Risk Mitigation

Organizations believe they're protected—then they try to restore data.

Backups are only valuable if they can be restored. Many organizations assume they're protected—but don't fully validate recovery until an incident occurs. When they do, issues like corrupted files, incomplete backups, or unclear processes can significantly delay recovery. This doesn't just impact IT—it affects revenue, operations, and customer trust.

What LP commonly sees during incidents & testing

Many organizations assume backups are functioning correctly but common issues discovered during testing and incident management include:

- Backups exist—but have not been tested end-to-end
- Recovery takes significantly longer than expected—sometimes days, not hours
- Key employees are unsure of their roles
- Backup schedules are not custom to systems / content types
- Critical systems are not thoroughly identified or prioritized correctly

Questions To Pressure-Test Your Backup & Recovery Plan Strategy

What data is critical to keep your business running?	Do you follow the 3-2-1- Backup Method?	Where are your backups stored—and are they protected?

The question isn't whether you have backups. It's whether you can rely on them when it matters.

Insurers Look For

✓ Evidence that backups are tested regularly

✓ Defined recovery time objectives

✓ Secure, segregated backup environments

✓ Protection against ransomware targeting backups

How LP Helps

✓ Advise on recovery gaps that could impact claim outcomes

✓ Align your recovery practices with evolving cyber insurance expectations

✓ Connect you with trusted partners to test and strengthen recovery plans