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

Level-setting of what this flyer is about

Overview Headline

Overview text

Software & Cyber Security

Add info about 3rd party software impacting company security

add stat about software leading to hacks/compromises or about average # of updates required for each piece of software each year

Tips on How to Get Started

- Add 3-5 quick tips on how to start ensuring software is current

Carrier insights / LP Offerings

- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering

Enforce Strong Access Controls

Cyber Risk Mitigation

Level-setting of what this flyer is about

Overview Headline

Overview text

Least-Privilege Policy

Add info about what this means, why it is recommended

add relevant stat

Tips on How to Get Started

- add tips - e.g., Set correct access standard for new employees upon new hire orientation.
- Review access of current and tenured employees annually.

Carrier insights / LP Offerings

- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering

Back Up Critical Data & Test Recovery Plans

Cyber Risk Mitigation

Level-setting of what this flyer is about

Overview Headline

Overview text

Ransomware

Add info about what this means, why restoration practices must be ready

add relevant stat

Tips

- add tips on backup systems, frequency for backups, frequency and types of testing recommended

Carrier insights / LP Offerings

- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering
- **Add insight/offering.** Describe insight/offering