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.