

# 10 STEPS TO STRENGTHEN YOUR CYBER-SECURITY



## 1. Risk Assessment

Conduct a comprehensive cybersecurity audit to identify potential vulnerabilities within the enterprise.

## 3. Update Regularly

Ensure all systems, software, and applications are updated frequently. Patches often address known security vulnerabilities.

## 5. Regular Backups

Backup essential data regularly to multiple secure locations, both on-site and off-site.

## 7. Install Security Tools

Utilize next-gen firewalls, EDR (preferred), AV (antivirus), and intrusion detection systems to identify and block malicious activities.

## 9. Incident Response Plan

Develop a clear and actionable response plan for potential breaches, ensuring quick containment and mitigation.

## 2. Employee Training

Educate staff regularly on cybersecurity best practices, recognizing phishing attempts, and the importance of strong password management.

## 4. Implement MFA

Require Multi-Factor Authentication (MFA) for accessing critical enterprise systems to add an extra layer of security.

## 6. Network Segmentation

Separate critical systems and data from the broader network to limit the spread of potential breaches.

## 8. Monitor Your Environment

Employ 24/7 security log and network traffic monitoring solutions and services like MDR to detect unusual, suspicious, or malicious activities or unauthorized access.

## 10. Vendor Vetting

Evaluate and monitor third-party vendors' cybersecurity practices to ensure they meet the enterprise's security standards and understand your supply chain risks.

**READY TO SECURE YOUR BUSINESS?**

Sign up for our Complimentary Vulnerability Assessment [HERE](#).