IGI Cybersecurity | nodeware®

PROACTIVE CYBERSECURITY: THE FOUR PILLARS

BUILDING A STRONG FOUNDATION FOR YOUR BUSINESS SECURITY

Protecting your business requires more than just reacting to threats after they occur. A proactive cybersecurity approach focuses on prevention and is essential for maintaining strong defenses, meeting compliance requirements, and qualifying for cyber insurance. Think of it as preventive healthcare for your business. Regular checkups and good habits keep your systems and people protected. The four pillars below represent fundamental practices that keep your systems healthy and secure.

EMAIL SECURITY

Email remains the most common entry point for cyber attacks. Advanced email security solutions detect and block phishing attempts, malware, and malicious links before they reach your inbox.

MULTI-FACTOR AUTHENTICATION (MFA)

Adding an extra verification step beyond passwords dramatically reduces the risk of unauthorized access. Even if credentials are compromised, MFA requires additional authentication to keep your accounts secure.

SECURITY AWARENESS TRAINING

Your employees are your first line of defense. Regular training helps your team recognize social engineering tactics, suspicious emails, and other threats, turning them into active contributors to your security.

VULNERABILITY MANAGEMENT

Regular scanning and patching of your systems identifies and addresses vulnerabilities before attackers can exploit them. This continuous process keeps your infrastructure resilient against emerging threats.

Why This Matters for Your Business

- ✓ Reduce the likelihood and severity of security incidents
- ✓ Protect against both external threats and insider risks
- ✓ Meet compliance requirements and security framework standards
- ✓ Qualify for and maintain cyber insurance coverage