IGI Cybersecurity | nadeware®

STRENGTHEN YOUR CYBERSECURITY

UNDERSTANDING VULNERABILITY MANAGEMENT & PENETRATION TESTING

Vulnerability management and penetration testing are two important security services. Though often confused for one another, they serve distinct purposes. Vulnerability management is the process of scanning for and patching vulnerabilities on an ongoing basis, while penetration testing simulates a real-world cyber attack to test your defenses. **Many cyber insurance policies and compliance frameworks now require both services.** Here's how each helps protect your business:

VULNERABILITY MANAGEMENT

Ongoing Protection
Continuous identification and remediation of vulnerabilities before they can be exploited.

Benefit:
Reduces cyber risk by eliminating vulnerabilities before attackers find them.

PENETRATION TESTING

Real-World Validation
Simulated cyber-attacks to assess how well your defenses hold up against actual threats.

Benefit:
Identifies blind spots in your defenses and reveals actual risk exposure.

QUICK COMPARISON

	VULNERABILITY MANAGEMENT	PENETRATION TESTING
OBJECTIVE	Identify and fix known vulnerabilities	Evaluate overall security effectiveness
FREQUENCY	Continuous (recommended)	Annually, at a minimum
SCOPE	Entire IT infrastructure	Specific systems, or all systems
APPROACH	Automated scanning + manual review	Simulated real-world attack

Why Both? Vulnerability management keeps daily threats at bay, while penetration testing validates that your defenses actually work against sophisticated attack techniques. Together, they satisfy compliance requirements and provide the comprehensive protection your business needs.