CyberWatch

An Independent Risk Assessment Guide

How Organizations Reduce Cyber Risk, Protect Operations, and Maintain Compliance Visibility

AFFILIATED

Cybersecurity, Compliance, & Managed IT Support

Introduction to **Cyber**Watch by Affiliated

In today's threat landscape, every organization faces sophisticated cyber risks that can disrupt operations, damage client relationships, and create compliance exposure.

While many organizations invest in cybersecurity tools and IT defenses, leadership often lacks independent visibility into whether those investments are working or where critical gaps remain.

That's why we developed **Cyber**Watch. By combining ongoing penetration testing, vulnerability assessment, and strategic security guidance, our goal is simple: give organizations clearer risk visibility so they can protect what matters most before disruptions happen.

This guide explains how **Cyber**Watch helps organizations understand their current security posture, prioritize remediation efforts, and demonstrate due diligence to insurers, auditors, and stakeholders.

Sincerely,

Mike Moran
President
Affiliated Resource Group
Columbus, Ohio

Secure Operations Depend on Clear Cyber Risk Visibility

Business systems, sensitive data, and daily operations all carry risk. Organizations depend on secure systems, protected information, and reliable operations to serve customers, maintain compliance, and protect profitability.

This is not just an IT issue. It is an operational, financial, and compliance issue.

When a cyber incident happens, it can affect:

- Email and productivity systems
- Payroll and finance operations
- Customer data and confidential information
- Microsoft 365 and Active Directory environments
- Regulatory compliance standing

Your team may never see the technical cause. They will feel the disruption immediately.

CyberWatch by Affiliated is a unique risk assessment service that discovers vulnerabilities in an organization's environment so they can be found and fixed before hackers do. It serves as an independent evaluation of security and compliance health.

That gives leadership and their cybersecurity solutions provider a clearer understanding of:

- Where you have cybersecurity exposures
- Where current protections are sufficient
- Where security spending matters most

What's at Stake for Your Organization

Every organization is at risk. Consider this, cyber crime:

To grow 15% over the next two years	Costs **$8 trillion** annually	**2,300+ occurs every day** in the US

An independent cybersecurity assessment is especially important for organizations that:

- Would face significant financial hardship if operations shut down for 48 hours because of ransomware or another hacker exploit
- Handle sensitive customer, employee, or financial information that must be protected
- Are subject to regulatory mandates and compliance expectations (SOC2, HIPAA, CMMC, FTC Guidelines, industry-specific requirements)
- Need to demonstrate due diligence in cyber defense and governance, risk, and compliance
- Need cyber insurance coverage to help mitigate financial and legal risk
- Must protect client confidence and avoid reputational damage following a cyber incident
- Serve corporate customers or partners that require supply chain security validation

Leadership wants to protect systems, data, and operations.

They also need a clearer view of current risk.

CyberWatch Gives Leadership a Clear View of Cyber Risk

CyberWatch is a unique risk assessment service that discovers vulnerabilities in an organization's environment so they can be found and fixed before hackers do.

It serves as an independent evaluation of security and compliance health. Similar to how you rely on regular health checkups to catch problems early, or how you trust health inspections to verify restaurant safety.

That gives your organization and your cybersecurity solutions provider a clearer understanding of:

- Where you have cybersecurity exposures
- Where current protections are sufficient
- Where security spending matters most

CyberWatch doesn't just list potential problems.

It includes expert analysis of discovered issues and vulnerabilities, along with prioritized remediation guidance—so your organization has a clear path to stronger cybersecurity, smarter spending, and greater operational confidence.

CyberWatch

- ✓ Keeps operations running
- ✓ Protects sensitive information
- ✓ Gives leadership an independent view of security & compliance risk

CyberWatch Goes Beyond Assessments

CyberWatch is not a one-time scan, annual checklist, or standalone penetration test. It is an ongoing, independent risk assessment and penetration testing program built to give organizations clearer visibility, stronger guidance, and continuous validation.

It not only uncovers unknown vulnerabilities and unnecessary risk, but gives your organization built-in access to Affiliated resources that help guide you forward so, findings turn into action.

CyberWatch can stand on its own as a complete independent security program or work alongside your existing IT and cybersecurity tools to add an extra layer of validation, accountability, and insight.

What **Cyber**Watch Includes:

- **Quarterly Penetration Testing**
  Ongoing testing that provides elevated visibility into evolving risks and exposures.
- **Remediation Planning & Security Strategy**
  Understand what to fix first, where to invest, and what matters most to protect
- **Dedicated Account Manager**
  A consistent point of contact to review findings, prioritize next steps, and keep momentum moving.
- **Monthly Remediation Tracking & Roadmap Updates**
  Ongoing status reviews that help ensure issues are addressed and progress stays visible.
- **Quarterly Security Strategy Briefing (vCISO)**
  Executive-level guidance to help leadership understand risk, priorities, and strategic next steps.
- **Executive Reporting**
  Clear reporting for organizational leaders, boards, and decision-makers.
- **Technical Findings for IT Teams**
  Actionable detail your internal team or provider can use immediately.

Clearer direction, stronger visibility, and more value from every assessment.

What **Cyber**Watch Tests

- Penetration testing that evaluates cyber defenses against phishing, insider threats, and supply chain attacks
- Inspection for internal vulnerabilities that evaluates cyber defense tools, system configurations, and technical security controls
- Review of external vulnerabilities to identify possible points of attack and measure the risk associated with discovered vulnerabilities
- Asset-specific assessments for Microsoft 365, Active Directory, and other commonly deployed IT systems
- Identification and review of personally identifiable information to help organizations understand where sensitive data exists and how vulnerable it may be

Why It Matters

The safest organizations are not always the ones that spend the most on security or have the largest teams.

The safest organizations use a reliable independent security service provider to continuously scan, test, and evaluate their environment to make sure they are safe.

CyberWatch helps organizations:

- Find vulnerabilities and give recommended fixes
- Confirm what is already working
- Demonstrate to insurers, auditors, and stakeholders that security and compliance are being taken seriously
- Operate with greater confidence

For more information and assistance, contact the CyberWatch team:

Affiliated Resource Group
614.495.9658
aresgrp.com

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support