CALIAN®

Cyber Security Solutions

3 STAGES OF CYBER SECURITY

Before a Cyber Security Incident Occurs

Training

Security awareness training is a top priority: teach employees about good password hygiene, how to look for threats and scams. Knowledge of security policies and procedures and how to mitigate risk is critical.

Penetration Testing

Work with professionals to stress test security systems from a hacker's perspective for insight into technology gaps and the role people play in a potential breach.

Discover Vulnerabilities
Understand current security shortfalls within the network and critical hosts and take action to secure them.

Get Remediation Advice
Obtain resolution instructions from experienced security experts.

Test Incident Response
Prepare the security team and test existing monitoring tools for attacks.

Maturity Assessment

Conduct a maturity assessment to mitigate risk; for instance, include an assessment of things such as:

- ✓ External & Physical Security Environments
- ✓ Microsoft Windows & Unix Environments
- ✓ Firewall
- ✓ VPN
- ✓ Server Configuration
- ✓ Network Architecture
- ✓ Wireless & Mobile Security
- ✓ VoIP Security (if applicable)
- ✓ Social Engineering Vulnerabilities

During a Cyber Security Incident

Key Indicators of Compromise (IoC) & Remediation

IoCs relate to the forensic data in systems while a breach is occurring such as system log entries and other file types that aid in detecting malicious code or unauthorized activities. When cyber security experts find IoCs, they can stop the breach and limit the impact.

After a Cyber Security Incident

Lessons can be learned from the after-effects of a breach or attack.

After-Action Review

An AAR looks at all aspects of the incident including how systems worked, how people reacted, what processes needed improvement, what new processes or technology should be implemented.

Tabletop Exercise

This is the next step. Take what was learned from the AAR, incorporate all updates and improvements to technology, processes, and training, then run a realistic simulation to test how everything works.

By taking part in these exercises, organizations can stress test everything under controlled conditions, avoiding mistakes when an attack occurs. Even if no attack has occurred, adding a tabletop exercise to the first phase is a perfect place to start.

CYBER.CALIAN.COM