

Preparing for Successful Vulnerability Management

Use this brief worksheet to gauge your organization's preparedness for implementing a successful vulnerability management program.

Vulnerability Identification

- What sources (e.g. mailing lists, websites) do you consult for information on vulnerabilities, security updates, and other security issues?
- Do you have an IT systems and/or asset management system that is capable of providing accurate IT asset inventory reporting?
- Do you perform periodic and regular vulnerability identification in your environment (e.g. vulnerability scanning, patch scanning, system auditing)?

Threat Prioritization

- Does your organization have a formal process for establishing the criticality of assets?
- What means do you have of establishing priority for security risks discovered in your environment (e.g. policy statements, vendor rankings of security issues and updates)?
- What process and/or tools are used to automate security updates (e.g. systems/desktop management software, patch management tools, login scripts)?

Change Management

- Do you have a formal change management process?
- Are security related changes (e.g. patches, configuration changes, firewall policy changes) handled through the change management system (including rollback plans)?
- Do you have a test environment for vetting security-related changes?

Risk Reduction

- Do you use formal techniques such as threat modeling and attack trees to diagram potential threats to your environment?
- Do you practice regular risk assessment for your business and IT assets?

Ensuring Compliance

- Is your organization subject to any external regulatory influences (e.g. HIPAA, CISP/PCI)?
- Does your security policy mandate security baselines (configuration requirements, etc.)?
- Do you regularly test compliance with external regulations and internal policy?

Lifecycle

- Do you have a means of tracking discovered vulnerabilities, relative risk, and other security-related metrics over time?

