GOTHAM
government solutions

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Comments: Submitted by Russell D. Vines, CISSP, CEH, PCI QSA, NSA-IAM, CISM, Security+, Chief Security Advisor to the office of the CTO, Gotham Technology Group, in response to the February 26, 2013 Request for Information Noticed by the National Institute of Standards and Technology (NIST)

Contact: William Blum, Federal Director, Gotham Government Solutions, LLC, 11951 Freedom Drive, Suite 1300 Reston, Virginia 20190, Office: 703.251.4469 | Cell: 571-276-6680 | Fax: 703.251.4470, bblum@gothamgs.com | www.gothamtg.com

Comments on the Framework

Our comment response to the RFI is composed of two parts:

1) Answers to specific RFI questions that Gotham has identified as most relevant to our involvement with cybersecurity, and;
2) General comments related to the NIST process itself.

Specific Comments

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

> Gotham sees the greatest challenge to cybersecurity as the lack of technical validation of risk controls, especially in the area of vulnerability assessment. (See General Comments below.) This validation is vital to determine the target's compliance stance.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

> The field of Information Systems currently has myrad standards and policies applicable to private commercial cybersecurity processes: ISO 27K, Cobit, HIPAA/HyTrust, PCI DSS, various CMMs, and many more that apply to Federal systems (historically, the Federal Governemt has been the intiator in securing systems.)

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

> For a firm such as Gotham, physical and information infrastructures such telecommunications, energy, financial services, and transportation sectors, are very critical in the function of our core business. Cybersecurity protections focused on critical infrastructure are a base requirement of our mission statement.

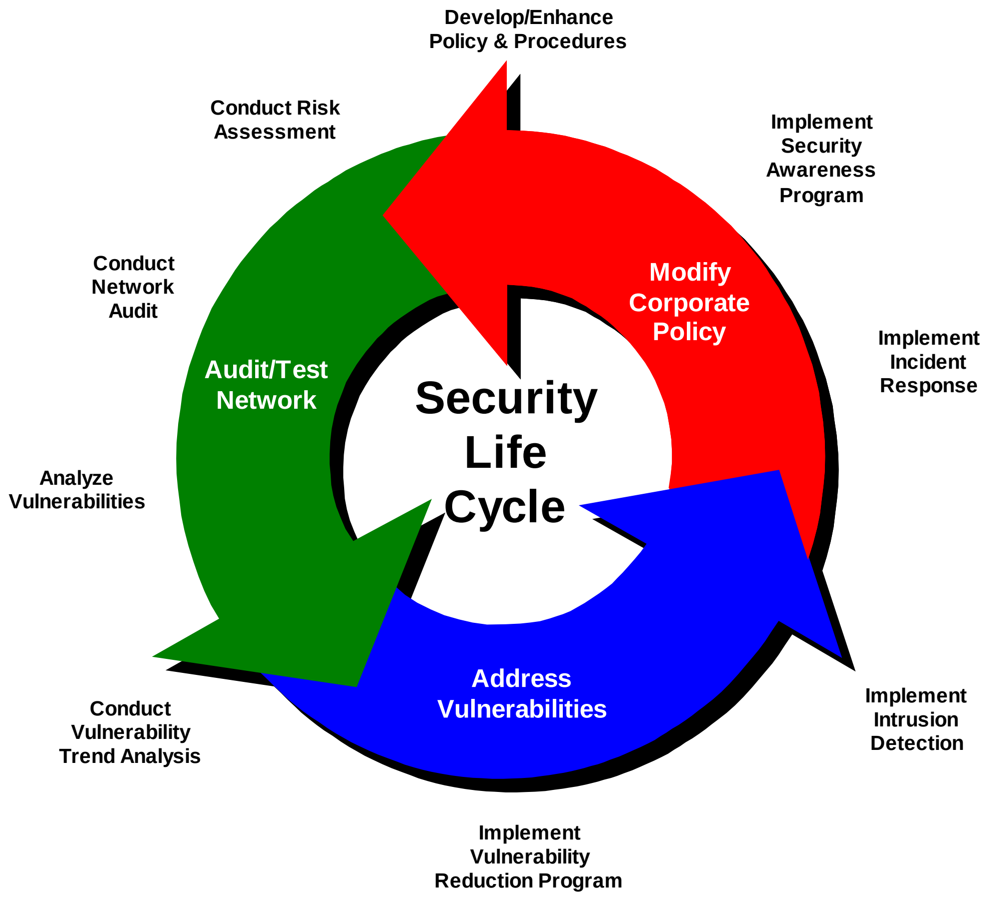
Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

> As Gotham is a certified PCI qualified Security Assessor, we have found that the PCI DSS is also useful as a base practice model for generic non-card holder systems, as it is derived from several other base and best practice standards.
>
> Another useful assessment process that Gotham uses is the IAM model of the Security Life Cycle. Though somewhat dated, the overall process describes a still useful lifecycle in improving an organization's security posture[1]:

[1] http://www.nsa.gov/index.shtml

The NSA IAM Methodology Lifecycle


Develop/Enhance Policy & Procedures
Conduct Risk Assessment
Implement Security Awareness Program
Conduct Network Audit
Modify Corporate Policy
Implement Incident Response
Audit/Test Network
Security Life Cycle
Analyze Vulnerabilities
Address Vulnerabilities
Implement Intrusion Detection
Conduct Vulnerability Trend Analysis
Implement Vulnerability Reduction Program

2. Which of these approaches apply across sectors?

The major advances in securing computer systems and networks have come through the information system technology route, with origins in computer science and software engineering. A large number of the personnel populating the systems controlling the critial infrastructure come from electrical, mechanical, and chemical engineering backgrounds. The motivations, requirements, and focus of each of these groups are not the same and differences have to be taken into account.

For example, the performance of a process in a plant is critical, and inadequate performance in production areas can result in huge financial losses, equipment damage, and personnel injuries. These severe consequences of operational errors are not usually a common occurrence in IT facilities. Similarly, safety is another very critical concern in a production environment.

6. How do these approaches take into account sector-specific needs?

> An important point to consider is the fundamental principles for protecting computer systems and networks are valid across all application domains. However, these principles have to be tailored to the systems used in the critical infrastructure to be effective in protecting these systems.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

> From experience and application of engineering approaches, a number of valuable standards and guidelines have been developed and documented for securing automation systems. These materials and the extensive effort involved in their generation should be seen as a resource that can be used as a basis for the development of the proposed framework.

General Comments

Gotham feels that the need for third-party verification of the security posture of an organization has to be a vital element of any complete security effort. This verification should come in the form of active technical assessment of the target based on the tenets of Ethical Hacking. These assessment activities should include:

- External and Internal Vulnerability Scanning, using both automated industry products and manual open source tools;
- Wireless and Voice Systems Assessments, as a large percentage of Wi-Fi, RFI , VoIP and older PBX systems still contain legacy vulnerabilitites;
- Social Engineering Exploits, as targeted spear-phishing campaigns are one of the oldest, yet still most effective vectors into an organization;
- Security Awareness training, one of the few options available to protect from phishing exploits;
- Virtualized Systems Assessment, as the explosion of virtualization to the desktop opens a new attack surface.