Office of the
Chief Information Officer

AFCEA

Eric Cole

Director, Cyber Security Oversight

U.S. Department of Energy

08/20/08

IT Normalcy Evolving

- Yesterday
  - Exploits were not as prevalent
  - Required high level of technical knowledge
  - Security was a specialty
- Today
  - Management is integrated into the solution
  - Security is built into investments at various levels
  - Everyone is a security advocate
  - Security is a key component to success versus an optional exercise

Effective Security Programs

- Iterative process
- Continual processes in place
  - Evaluation
  - Revision
  - Updating
- Reflects management's risk tolerance

Hybrid Security Approach

- Reduction in the cyber threat

AND/OR

- Reduce system vulnerabilities to threats

Threats

- External
  - Hackers
  - Virus
  - Non-virus malicious software (worms)
  - Social engineering
- Internal
  - Collusion
  - Abuse of privileges
  - Cover-ups

Security Requirements

- Requirement is NOT to prevent every exploit

- Requirement is to:
  - Know the vulnerabilities that exist
  - Identify what is worth protecting
  - Deter threats
  - Determine acceptable risks
  - Monitor system activity
  - Detect and prevent inappropriate behavior

Defense-in-Depth Goal

- Balance security with cost effective solutions

- What approach is required to defend information from unauthorized disclosure or loss?

Organizational Controls

- Isolate functions associated with information from the larger business entity when possible
- Ensure activities not related to the data requiring protection are not affected
- Protect rest of the organization from being subjected to unneeded requirements

Policies and Procedures

- Documentation is not a one time only exercise
- Define the systems requirements for processing
  - Revisit when significant changes occur
  - Revisit after a certain passage of time
  - Allow for modernization
- May include
  - Formal certification and accreditation processes
  - Requirements defined by law

What can vendors do?

- When developing solutions vendor could
  - Understand the NIST 800 series world the government operates in
  - Build in controls identified in 800-53
  - Document all safeguards

What can all security professionals do?

- Advocate implementing 2-factor authentication for every user in the enterprise

- Understand the difference between reducing the threats versus reducing the vulnerabilities

What can everyone do?

- A tendency exists to gravitate to toward the technologies we are familiar with.
  - Must be aware of our own technical prejudice
  - Must facilitate discussions with individuals from diverse backgrounds
- Ask, do we have more than one system performing like functions and are they needed?

What can everyone do?

- Discuss the creation of a risk profile for assets, programs, individuals, etc. based on specific risk categorizations
  - Example: Tracking assets like BBs and PCs of managers and HR professionals likely to contain PII

Keys to Technical Success

- Avoid dictating certain technologies and encourage implementation measures appropriate for the environment
  - Flexibility to the point that it can address all aspects of security
  - Scalable to entities of any size
  - Technologically neutral