Forensics and Active Protection

Computer and Network Forensics Research Project
2003 Work Update

Yanet Manzano
Florida State University
manzano@cs.fsu.edu

Outline

- CNF Project Goal Review
- Presentation Goal
- Information Security Policies Review
- Security Risk and Control Review
- ISO 17799
- National Strategy to Secure Cyberspace
- Conclusion
CNF Project Goals Review

Computer and Network Security Project Goals

- Help enterprises deter computer crime
- Improving their ability to conduct CNF analysis

**Presentation Goal:**
Updates on key issue relevant to CNF policies

Information Security (IS) Policies

**COVERAGE**

cover the full range of risks associated with creating, amending or storing information

- Securing Hardware, Peripherals and Other Equipment
- Controlling Access to Information and Systems
- Processing Information and Documents
- Purchasing and Maintaining Commercial Software
- Developing and Maintaining In-house Software
- Combating Cyber Crime
Information Security (IS) Policies

COVERAGE

- Complying with Legal and Policy Requirements
- Planning for Business Continuity
- Addressing Personnel / HR Issues Relating to Information Security
- Controlling e-Commerce Information Security
- Delivering Training and Staff Awareness
- Dealing with Premises Related Considerations
- Detecting and Responding to Security Incidents
- Classifying Information and Data

IS policy: intended to support the protection, control and management of info assets

- protect business and client or customer info
- establish responsibility and accountability for IS
- maintain management and staff awareness, knowledge and skill
- ensure commercial activities in the event of significant IS incident
- Meet standards
IS Policies

SCOPE

**Covers all info assets:**

- Stored
  - databases, or computers
  - removable media such as CD-ROMs
  - fixed media such as hard disks and disk sub-systems

- Transmitted
  - across internal and public networks

- Spoken during telephone calls and meetings or conveyed by any other method (email)

---

Security Risk (SR) Analysis Review

- essential in ensuring controls and expenditures are equivalent to the risk to the enterprise is exposed to

- **Threats** create attacks

- Attacks exploit **Vulnerabilities**

- **Controls** are countermeasures for vulnerabilities
Security Controls (SC) Review

- **Deterrent**
  - reduce likelihood of deliberate attack

- **Preventative**
  - detect and eliminate vulnerabilities

- **Corrective**
  - reduce effect of attack

- **Detective**
  - detect attacks
  - trigger preventative or corrective controls

SR and SC Relational Model
ISO 17799: International Security Standard

- A comprehensive set of controls comprising best practices in information security
- Single reference point for identifying a range of controls needed for more situations where information systems are used in industry and commerce
- Standard relevance as a common currency for information security measurement
- Main standard being used for security policy development

Large Enterprises
Toward a Corporate Security Council

- consisting of key members of the company with security-related responsibilities
- Officials can
  - prepare and coordinate plans to ensure cybersecurity is factored into enterprise and business operations
  - advise the CEO in a crisis
  - coordinate the execution of their contingency and continuity plans in response to cybersecurity incidents

Best Practices

- facilitate the integrity, reliability, availability, and confidentiality of the enterprise
- Authentication: Implement processes and procedures to authenticate, or verify, users of the network
- Configuration management: enterprise architecture and deployment with security in mind
  - enterprise wide software, patches, and OS control
Best Practices

**Training:** Train all employees on the need for IT security
- Develop policies based on roles
- Verify compliance
- Periodic Reviews

**Incident response:** Develop enterprise capability for
- responding to incidents
- mitigating damage
- recovering systems
- investigating and capturing forensic evidence
- working with law enforcement

Best Practices

**Organization network:** Organize enterprise security, IT, and risk management functions to promote efficient exchange of information corporate-wide

**Network management:** Create a regular process to assess, remediate, and monitor the vulnerabilities of the network
- automated processes for vulnerability reporting, patching, and detecting insider threats.
Conclusion

- Policy-driven approach to managing info security
- Automate technology implementation and ongoing maintenance of key security management functions to
- Comprehensive security management integration and coverage enterprise wide
- Embed security in enterprise culture, business and technical operations