Sharon Hope's Lecture Notes

Sharon Hope's Lecture Notes for:
IEEE/PES All Councils Conference, subtitled The Power of the IEEE
Saturday, June 10, 7:30 to 4:00, at the Universal City Hilton Hotel
(One of 2 or more speakers from 10:30 - 11:30. Estimated 15 minute talk + Questions)

Specific Presentation by Sharon Hope:

Applying Y2k Teams to IT Security Issues

Newspaper Cartoons: 1: From Y2K, 2: I Love You Virus

Lessons from Y2K

Congratulations to Y2K Veterans!
Government & Industry vs common threat
- Largest joint effort since WWII
- Largest peacetime effort in history
CIO into the spotlight
Recognition of IT as central to infrastructure

IT Process

Top down imperative
Triage = System engineering of entire business
Work Internal and external dependencies
- IT equipment firmware
- Application Software
- OS
- Data
Standard Practice
- Awareness
- Inventory
- Assessment
- Renovation
- Validation
- Implementation
- Plus: Contingency Planning
Responsive to volatile information
- Additional vulnerabilities
- COTS bug fix releases

ITS is a Growing National Concern for Government & Private Sector

S. Hope, 6 June 2000, Applying_Y2K_Teams_to_Security_
Sharon Hope's Lecture Notes

News items, Legislation, National Policies

GAO Suggestion in October 99: CRITICAL INFRASTRUCTURE PROTECTION
Comprehensive Strategy Can Draw on Year 2000 Experiences

Larger threat than Y2K
  Virus & hackers
  Disgruntled Employees
  Industrial Espionage
  Cyberterrorism

Summarize Y2K similarity points for top-down security initiative.
  2 Billion$ budget requested
  Requires same top-down approach
  Best Practices & lessons learned from Y2K
  ITS Initiative – Govt & Business

Publicly Available Resources/Info
  General:
    • Government: White House and Congress
    • Bills, Testimony, State of Union Address
    • Call for Govt & Industry vs new threat

  Government URLs:
    • NIST
    • GAO
    • OMB
    • Etc.

  Commercial Resources
    • ITAA Newsletter
    • Magazines
    • Websites
    • Email Subscriptions
    • Training & Certification

S. Hope, 6 June 2000, Applying_Y2K_Teams_to_Security_
Applying Y2K Teams to IT Security Issues

Sharon Hope

for the IEEE/PES All Councils Conference

10 June 2000
Show Post-Y2K Cartoon
Lessons from Y2K

♦ Congratulations to Y2K Veterans!
♦ Government & Industry vs common threat
  – Largest joint effort since WWII
  – Largest peacetime effort in history
♦ CIO into the spotlight
♦ Recognition of IT as central to infrastructure
IT Process for Y2K (1 of 3)

- Top Down Approach was Imperative
- Triage = System Engineering of Enterprise
- Manage Internal and External Dependencies
  - IT Equipment Firmware
  - Application Software
  - OS
  - Data
  - External Interfaces
  - Supply Chain
IT Process for Y2K (2 of 3)

♦ Standard Practice
  - Awareness
  - Inventory
  - Assessment
  - Renovation
  - Validation
  - Implementation
  - Plus: Contingency Planning
IT Process for Y2K (3 of 3)

- Respond to Volatile Information
  - Additional Vulnerabilities Discovered
  - COTS Bug Fix Releases
- Eliminate Massively Redundant Activities
- Enforce Best Practices
  - Test
  - Configuration Management
Here are all of your holiday shopping bills, right on time.

Where's a Y2K glitch when you need one?
IT Security a Growing National Concern for Government & Industry

- News items, Legislation, National Policies
- Larger threat than Y2K
  - Virus & Hackers
  - Disgruntled Employees
  - Industrial Espionage
  - Cyber Terrorism
- National Plan for Information Systems Protection

FY 2000 Federal Budget Target: $2 Billion
GAO: Comprehensive Strategy Can Draw on Year 2000 Experiences (1 of 2)

- Y2K has laid a foundation for longer term improvements in the way we view, manage, and protect computer systems supporting our nation’s critical infrastructures. These areas include:
  - providing high-level congressional and executive branch leadership,
  - understanding risks to computer-supported operations,
  - providing adequate technical expertise,
  - providing standard guidance,
GAO: Comprehensive Strategy Can Draw on Year 2000 Experiences (2 of 2)

- establishing public-private sector relationships,
- facilitating progress and monitoring performance,
- developing an incident identification and coordination capability, and
- implementing fundamental information technology management improvements.

These factors...should be considered when developing a national strategy for critical infrastructure protection.
Resources: Government URLs

White House:

Congress:  http://www.house.gov/science/106_hearing.htm#Technology and
http://www.senate.gov/~judiciary/techterr.htm


♦ GAO:  http://www.gao.gov/audit.htm

♦ DOJ:  http://www.usdoj.gov/criminal/cybercrime/


♦ Dept. Commerce:  http://www.ecommerce.gov/

10 June, 2000  Sharon Hope: Applying Y2K Teams to IT Security Issues
Resources: Commercial

- ITAA Email Newsletter
- Year 2000 Email Newsletter
- Magazines
- Websites
- Email Subscriptions
- Training & Certification