

Overview of the Draft National Strategy to Secure Cyberspace

John Resotko

Head of Systems Administration

MSU-Detroit College of Law

The National Strategy to Secure Cyberspace

- Published by President's Critical Infrastructure Board in Sept. 2002
- Strategy as an ongoing process: comments due by Nov. 18, 2002
- Designed to supplement strategy documents for Homeland and National Security
- Not intended as a replacement for the normal budget policies

Core Components

- The Case For Action: Cyberspace Threats and Vulnerabilities
- Guiding Policy and Principles
- Highlights of the Strategy
- Five Levels of the National Strategy
 - Recommendations
 - Programs
 - Discussion Areas

A Case For Action

- Nation dependent on Cyberspace
- A range of known and developing threats
- Opportunity cost of securing systems
- Government alone cannot secure
Cyberspace: all levels must be responsible
- Need to raise awareness, share information,
protect and secure critical infrastructure

National Policy and Guiding Principles

- Embrace Private-Public Partnerships
- Avoid Regulation
- Safeguard Civil Liberties and Privacy
- Coordinate with Congress
- Cooperation with State and Local Governments

Guiding Strategic Principles

- Secure Parts to Secure the Whole
- Evolve measures to keep head of threats
- Empower all Americans through:
 - Awareness and Information
 - Technology and Tools
 - Training and Education
 - Roles and Partnerships
 - Federal Leadership
 - Coordination and Crisis Management

Audience Levels

- Level 1: the Home User
- Level 2: Large Enterprises
- Level 3: Government, Private Industry, and Higher Education
- Level 4: National Issues and Efforts
- Level 5: Global Issues

Audience Level Agenda Outline

- Recommendations: specific actions to promote Cybersecurity
- Programs: Existing efforts for the specific level audience
- Discussions: issues highlighted for additional analysis, debate, and discussion

Level 3: Higher Education

- Make IT security a priority
- Revise institutional security policy and improve use of existing tools
- Improve security for future research and education networks
- Improve collaboration w/industry, gov.
- Integrate our work with the national effort

Recommendations

Higher Education

- Consider establishment of a single point of contact in the event of cyber attacks.
- Create Information Sharing and Analysis Center (ISAC) to deal with attacks
- Create guidelines for “CIO”s and best practices for IT security
- Create model user awareness programs

Programs: Higher Education

- EDUCAUSE / Internet2 Task Force on Computers and Network Security
- National EDUCAUSE Workshop series with the National Science Foundation
- EDUCAUSE Outreach and Awareness programs to leaders and associations in higher education

Discussions: Higher Education

- What merit to adopting a model set of authorities for CIOs?
- Should federal funding be tied to compliance with cybersecurity guidelines?
- Should a central ISAC for higher education institutions be established?
- Should consider adoption of NIST Information Technology Security Assessment Framework?

Summary

- Emphasis on education, best practices, and strong policy at all levels.
- Improve communications and cooperation, ISACs and public-private partnerships
- Federal, State, and Local Governments to assess current security and IT system issues, and make addressing them a priority

Summary (continued)

- Set National priorities to accelerate the adoption of more secure systems, and improve security on Distributed Control systems related to critical infrastructure
- Continue to foster research in security, and encourage improved security in emerging systems

Summary (continued)

- Make Awareness, education, training, and certification in security a national priority
- Encourage market forces and voluntary, industry led vulnerability remediation
- Set national priorities for detection, analysis, and coordinated investigation and prosecution of cybercrimes

Industry Response

- “Companies should all do their part – that’s nice if you have money.” Ira Parker of Genuity, at a Cato Institute roundtable discussion 9/24/02
- “...we can’t leave the (security) problem to be solved through corporate belief in community responsibility or enlightened self-interest because we don’t believe such things generally exist in corporate circles.” Mark Gibbs, Network World magazine contributing editor

Responses (continued)

- What if vendors were liable financially for security problems? That would be an interesting question..” Steve Bellovin, researcher and one of the Internet Engineering Task Force directors
- “We’ve stepped up the cooperation between industry and government. This is the real beginnings of the dialogue.” Douglas Sabo, Network Associates director of government relations

Additional Resources

- White House site for draft policy and feedback : www.securecyberspace.gov
- EDUCAUSE security home: www.educause.edu/security
- SANS Institute: www.sans.org