# Market Incentives to Improve Cybersecurity

Herb Lin
National Research Council
INFORMATION SECURITY
AND PRIVACY ADVISORY BOARD
July 14, 2011

# The problem

- Cybersecurity is not just a matter of having good technologies and processes/procedures for cybersecurity.
- Cybersecurity measures must be deployed and used on a scale commensurate with plausible attacks.
- Economic and regulatory issues have some influence over deployment and use.

# Symptoms/drivers

- Cybersecurity as individual or organizational risk management results in a national cybersecurity posture that is far weaker than that needed by the nation as a whole. Individuals/organizations do not bear the full cost of catastrophic failures.

- COTS components are less secure because of low demand –
  - features and performance >> security
  - customer appreciate speed, ease of use, functionality, more thatn security

- Security usually imposes added cost, diminished performance (e.g., slower response times), inconvenience in use, and the awkwardness of monitoring and enforcement of security policies

- Recall failure of the U.S. government's Orange Book program.
  - government demanded secure systems
  - industry produced them
  - government agencies refused to buy them because they were slower and less functional than other nonsecure systems

# Possible solutions abound, including…

- Liability that subjects software and system vendors and system operators to potential damages for system breaches.
- Mandated reporting of security breaches that could threaten critical societal functions.
- Regulation that imposes best practices on system operators of critical infrastructure under threat of civil penalty.
- Accounting practices that force companies to report their cybersecurity practices and postures and the (sanitized) results of independently conducted red team attacks.
- ISO certification about conformance to relevant cybersecurity standards that can be used as a marketplace differentiator.

NO CONSENSUS ON THE RIGHT WAY TO PROCEED!

# A possible NRC study…

- Nature and extent of market failure (if any) to promote cybersecurity,
- Illustrative cybersecurity best practices that could improve the cybersecurity posture of various entities (e.g., individuals, providers of critical infrastructure, large and small organizations providing noncritical goods and services)
- Mechanisms that might be used to promote market mechanisms that to enchance national-level cybersecurity.
- Assessment of mechanisms above.
- Recommendations if possible.

# For more information…

Herb Lin

Computer Science and Telecommunications Board

National Research Council

hlin@nas.edu

202-334-3191