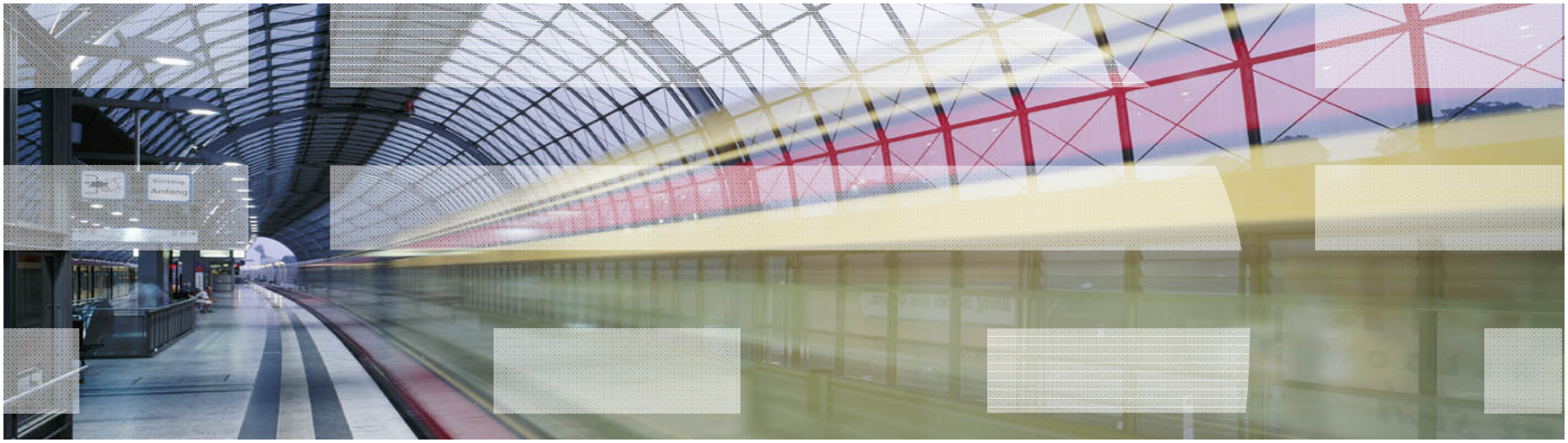
Threats and Key Issues for Cyber Workforce Training

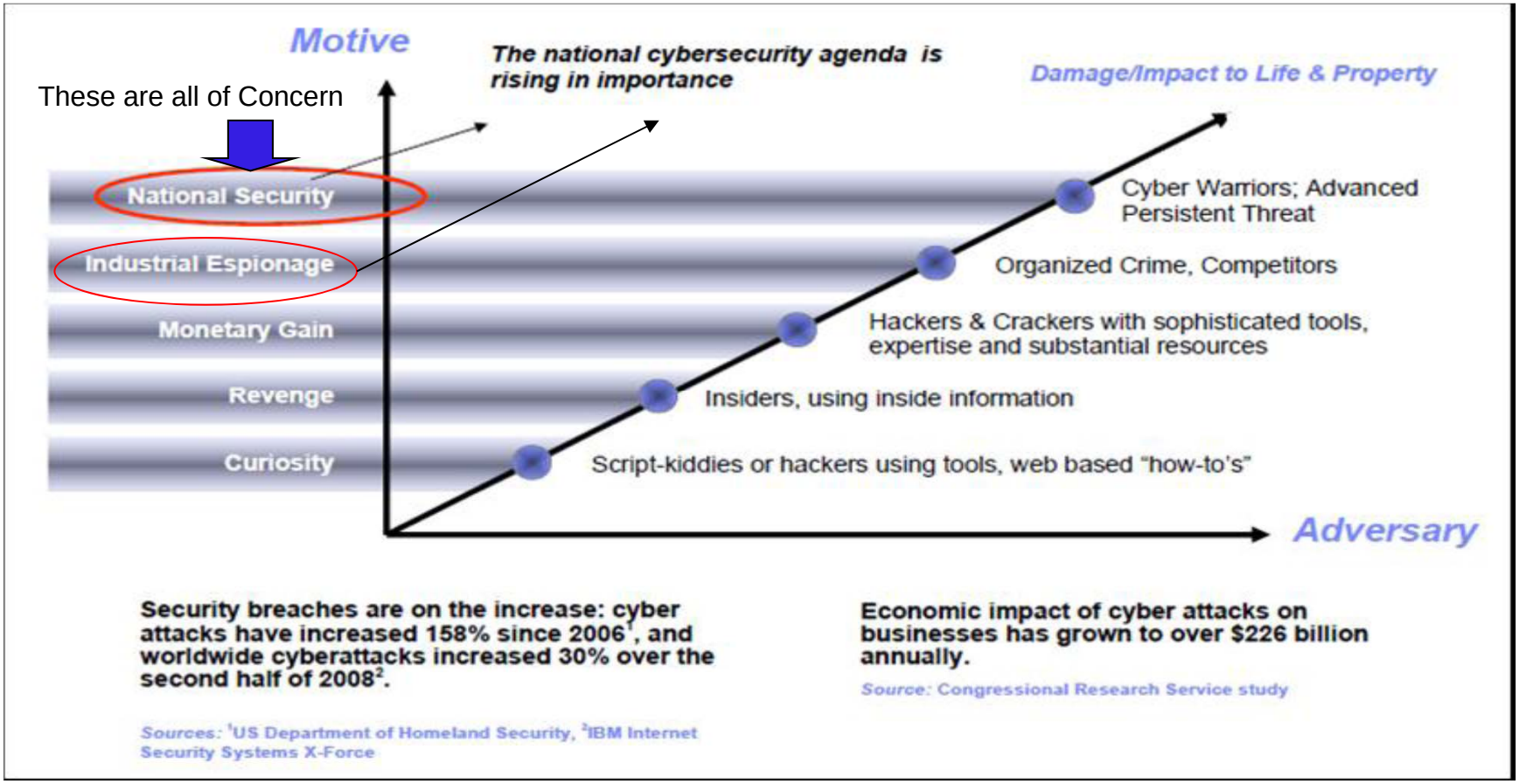
22 September, 2011

Dan Chenok,

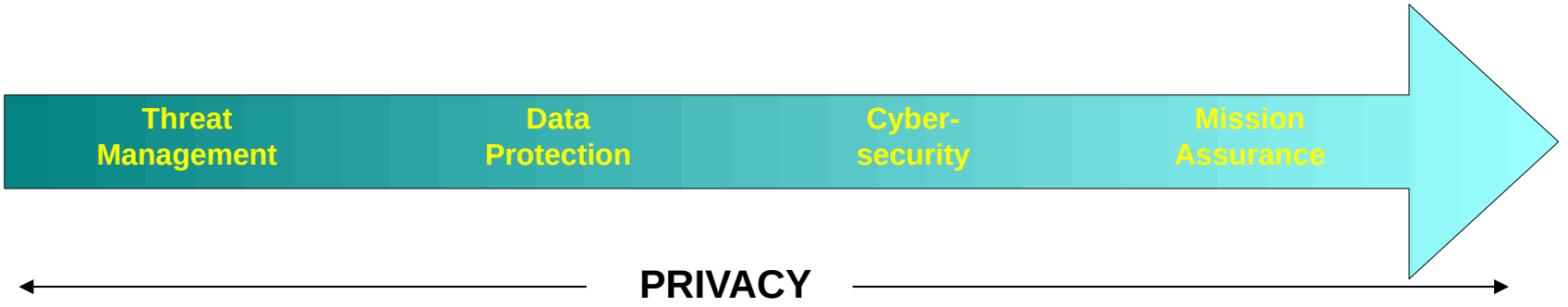
Senior Fellow, IBM Center for The Business of Government
Chair, Federal Information Security and Privacy Advisory Board



Cyber-Threats Are Becoming More Sophisticated



The concept of “cybersecurity” continues to evolve; U.S. federal agencies on maturation path from “react/protect” to “mission assurance”



- **Threat Management** – Identify/respond to computer network exploitation (CNE) and computer network attack (CNA)
- **Data Protection** – Threat management plus additional measures to prevent data loss, damage, and corruption and protect data even if it is lost
- **Cybersecurity** – Defensive measures to protect systems plus response and recovery; broadly includes more than IT, but also defensive measures around people, processes, policies
- **Mission Assurance** – Focus on holistic approach to proactively managing all aspects of IT and IT-related process and human capital that are critical to carrying out organizational mission. This approach results in a broader risk management approach and broadens discussion from tactics to strategy and from IT to all critical IT-related business processes and governance.
- **Privacy** – Permeates all aspects of cyber ; protection of personally identifiable information is essential in all phases

Key Cyber Issues Facing Federal Agencies

- Most important security issues facing Federal systems:
  - IT asset identification and system access
  - Trusted identity; roles based authentication; insider threats
  - Application security
  - Continuous monitoring
  - Situational awareness
  - Vulnerability management
  - Security metrics and dashboards
  - Data breaches/privacy
  - Secure cloud/FedRamp

IMPLICATIONS

- General agreement that bulk of spending on certifying/accrediting (C&A) IT systems must give way to a more operational posture of continuous monitoring
- Surveillance programs, including CYBERCOM and Einstein, may involve the potential for "active" responses by the U.S. in cyberspace
- Privacy and civil liberties concerns – come to fore given greater government monitoring of threats and activity, including on commercial networks
- High scrutiny on security of IT products and IT supply chain integrity

Lots of Policy and Legislation Afoot as a Result – Need to Know

- Legislation:
  - Senate: Lieberman-Collins, Rockefeller-Snowe, and Reid
  - House: Goodlatte, Lundgren, and Thornberry
  - Administration's Bill

- Policy:
  - CNCI and its progeny
  - Cyberspace Policy Review and its progeny
  - National Strategy for Trusted Identities in Cyberspace (NSTC)

- Lead Agencies
  - NSS – Cyber Coordinator
  - DHS -- NPPD
  - Commerce -- NIST
  - DOD – Cybercommand, NSA

Educating the Federal and Contractor Workforce

- NICE!
- Regular review of response to threats
  - Tips of the Day
  - Cyberscope reviews
- Continuous Monitoring
  - iPost
  - Cyberscope
- Different Focus for Different Folks:
  - Cyber team
  - IT team
  - Program officials
  - Executives