

The Austin Forum on Science, Technology & Society presents

Cybersecurity Today: Trends, Risk Mitigation & Research

Panelists

Joe Anthony, IBM

Dr. Fred Chang, UTSA

Ronald Perez, AMD

Moderator

Brad Englert, CIO UT Austin

./ 2011--Year of the Breach

Hackers continue to organize, taking aggressive political positions.

Cybercrime is targeting large volumes of personally identifiable data across a variety of markets.

At the same time, state sponsored cyber-attacks are on the rise.



CYBERSECURITY--A GLOBAL SOCIETAL ISSUE

./ Targets in the news

- Epsilon – Contacts from 100+ major companies exposed
- RSA – SecurID technology exposed
- Comodo – Spear-phishing led to attacker's ability to masquerade as a number of major Internet companies
- Sony Playstation – 100M customers exposed, 20K credit cards exposed.

./ Hacktivism

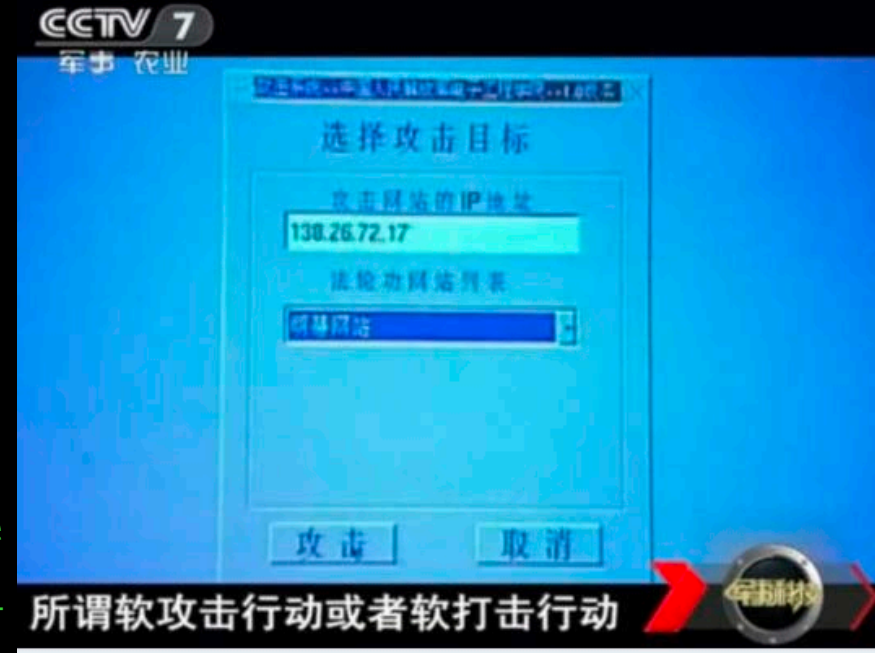
Anonymous, LulzSec &
Chinaeagle Union..

- Target low hanging fruit
- Collaborative,
international hacktivism
- Dozens of hacktivist
incidents this year



./ State Sponsored

- Operation 'Shady Rat' breached networks of 72 organizations across the globe
- Pentagon suffered most significant breach ever (24,000 classified files)
- 'Aurora' attacks targeted Cisco, Juniper, Google, & Adobe
- 'Night Dragon' attacks targeted global oil and gas data
- Continuing threat from cyber attacks on infrastructure (9/11 Commission recommendation unfulfilled)
- Cyber-attacks are now considered an "**Act of War.**"



./ UT Austin

- In 2010, the number of events involving university business systems increased by 28% as compared to 2009.
- The number of events involving personally owned or managed systems increased by 42% as compared to 2009.
- 2005 had previously been the “busiest” year with respect to the number of events, yet 2010 yielded 26% more events than were identified in 2005.
- At this point in 2011, UT Austin could surpass the number of events experienced in 2010.



Building a
Smarter Planet

Managing threats in the digital age

Joe Anthony
jca@us.ibm.com

September 2011





Security has moved from an IT issue to an ongoing business concern



Internal abuse of key sensitive information

WIKILEAKS

Unauthorized release of classified records

IMPACT

Close to \$100M for the U.S. Army alone; damaged foreign relations worldwide



Complexity of malware, ability to slowly leak data and affect critical business processes

STUXNET

Targeted changes to process controllers refining uranium

IMPACT

Degraded ability to safely process and control highly volatile materials



External data breach of third party data and theft of customer information

EPSILON

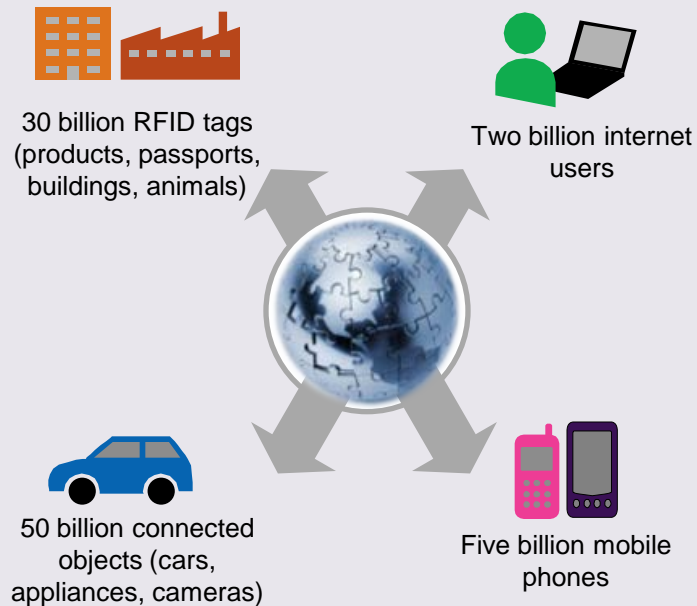
Theft of customer data affected > 100 companies

IMPACT

Up to \$4 billion in costs for initial clean-up and longer term litigation risks

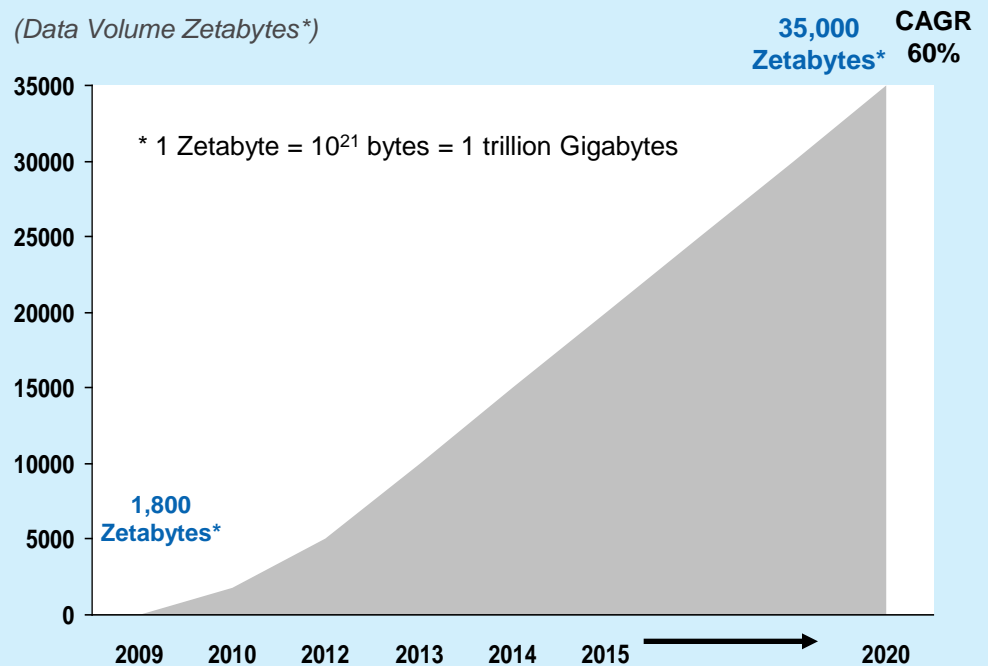
The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks

EXPLODING DIGITAL UNIVERSE



WORLDWIDE DATA VOLUMES PROJECTED TO INCREASE 29X OVER 10 YEARS

(Data Volume Zetabytes*)

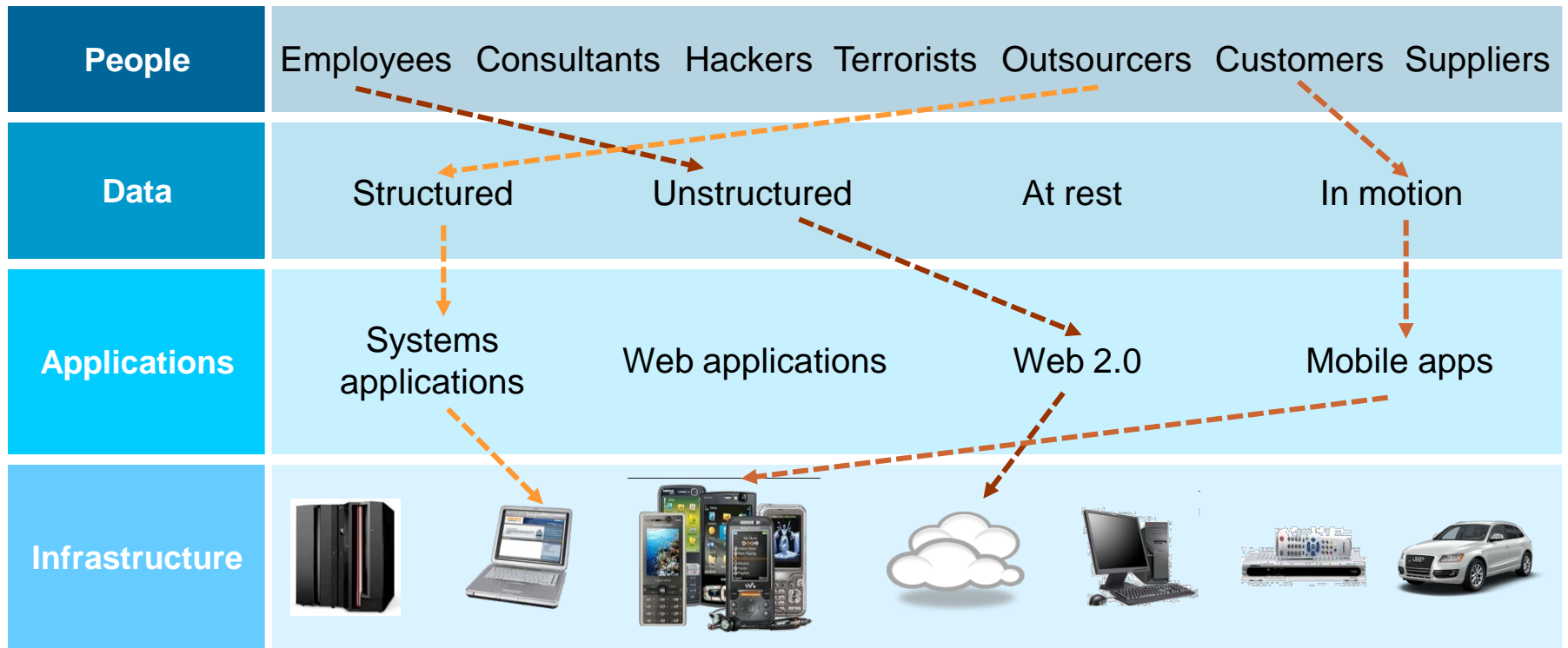


“There are security leaks involving mobile browsers that we don’t even know enough about yet.”

- CIO, Media Company

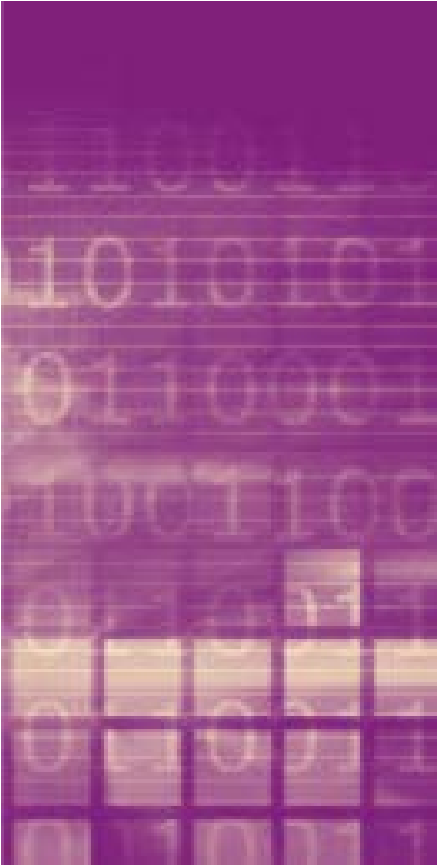
*Source: International Telecommunications Union. “Global Number of Internet Users, total and per 100 Inhabitants, 2000-2010.” United Nations. http://www.itu.int/ITU-D/ict/statistics/material/excel/2010/Internet_users_00-10_2.xls; Ericsson. “More than 50 billion connected devices – taking connected devices to mass market and profitability.” February 14, 2011. http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c; IDC “Digital Universe Study”, sponsored by EMC. May 2010

The attack surface is growing at an exponential rate



- **77%** of firms feel cyber-attacks harder to detect and **34%** low confidence to prevent
- **75%** felt effectiveness would increase with end-to-end solutions

Security challenges are increasing in number and scope...



EXTERNAL THREATS
Sharp rise in external attacks from non-traditional sources

- Cyber attack
- Organized crime
- Corporate espionage
- Government-sponsored attacks
- Social engineering

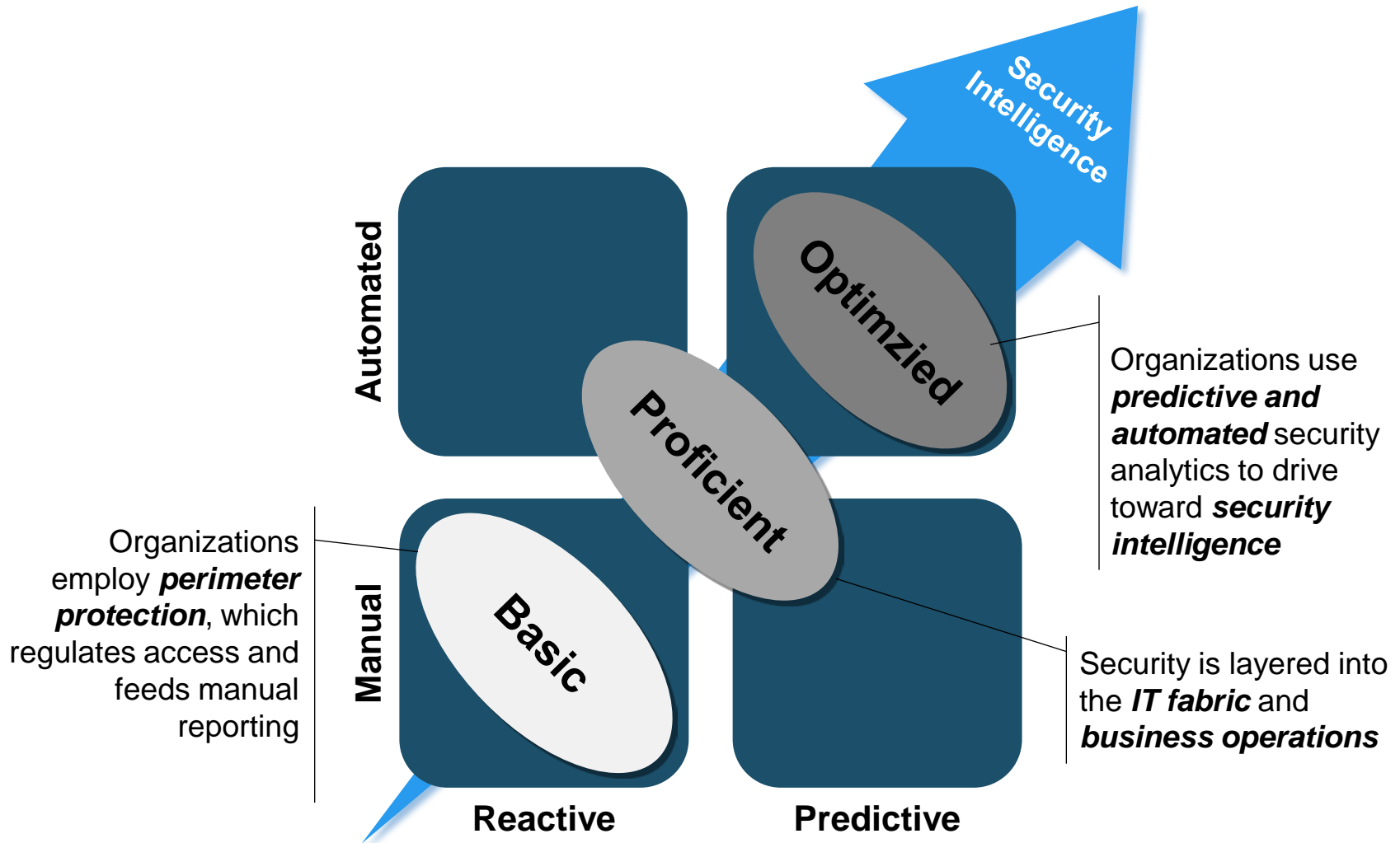
INTERNAL THREATS
Ongoing risk of careless and malicious insider behavior

- Administrative mistakes
- Careless inside behavior
- User breaches
- Disgruntled employees actions

COMPLIANCE
Growing need to address a steadily increasing number of mandates

- National regulations
- Industry standards
- Local mandates

Increased threats and compliance requirements require more automated, proactive approaches to security...





Cybersecurity Today: Trends, Risk Mitigation and Research

**The Austin Forum
Austin, TX
September 6, 2011**

**Frederick R. Chang, Ph.D.
AT&T Distinguished Chair in Infrastructure Assurance & Security
University of Texas at San Antonio**

Commission on Cybersecurity for the 44th Presidency

Securing Cyberspace for the 44th Presidency

A Report of the
CSIS Commission on Cybersecurity for the 44th Presidency

Cochairs:
Representative James R. Langevin
Representative Michael T. McCaul
Scott Charney
Lt. General Harry Raduege, USAF (Ret)

Project Director:
James A. Lewis

Center for Strategic and International Studies
Washington, DC
December 2008

Congressional
Sponsors:

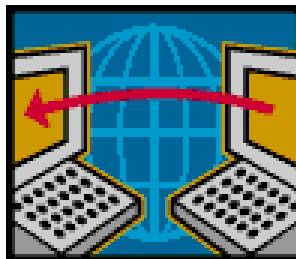
James Langevin (D-RI)

Michael McCaul (R-TX)

Human Capital Crisis in Cybersecurity

Estimate that there are only about 1,000 people in the U.S. who have the highly technical, specialized security skills to operate effectively in cyberspace -- need 20 to 30 times that many.

(From interview with Jim Gosler, Sandia Fellow, on NPR, July 2010)



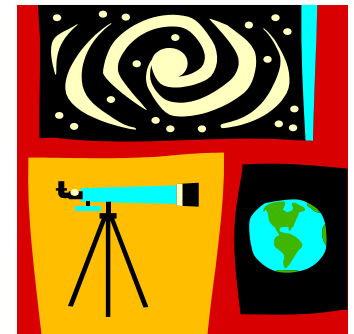
Human Capital Crisis in Cybersecurity

NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION (NICE)



Science of Cybersecurity

- Field is too ad-hoc and after-the-fact
- Lack a rigorous set of metrics
- Require a solid scientific basis
- Broad interdisciplinary approach





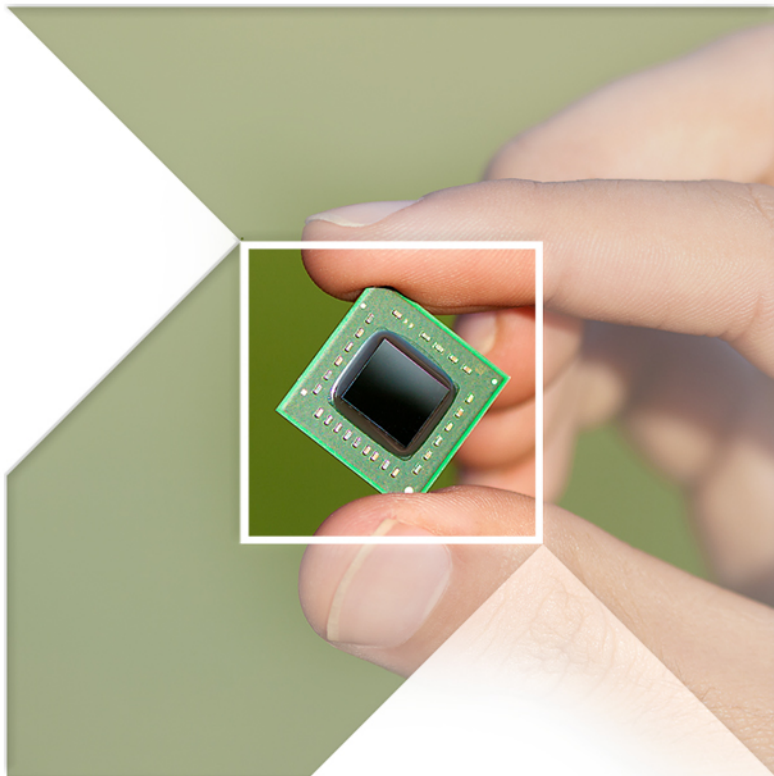
Science of Cybersecurity

NSF/IARPA/NSA Workshop on the
Science of Security

17-18 November 2008

Berkeley, CA

Science of Cyber-Security report
JASON Program Office
The MITRE Corporation
November 2010



CYBERSECURITY R&D: AN INDUSTRY PERSPECTIVE

*Cybersecurity Today:
Trends, Risk Mitigation and Research*

Ronald Perez
AMD Fellow, Security Strategy & Architecture

September 6, 2011



Industry Hears a Call for Public-Private Partnerships

"Working in partnership with the communities represented here today, we will develop a new comprehensive strategy to secure America's information and communications networks."

- President Barack Obama, May 29, 2009



[Home](#) | [NITRD Program](#) | [NITRD Groups](#) | [NITRD Events](#) | [PCAST](#) | [NCO](#) | [Laws](#) | [Publications](#)

NCLY Summit

NATIONAL CYBER LEAP YEAR SUMMIT 2009

August 17-19, 2009
Crystal Gateway Marriott
1700 Jefferson Davis Highway
Arlington, Virginia 22202

How do the Partners View Cyber Security R&D?



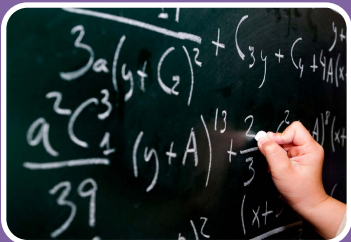
Government

- Invests primarily in R&D that is critically important to the security of the nation but cannot ensure the commercial applicability and productization of the technologies developed.



Industry

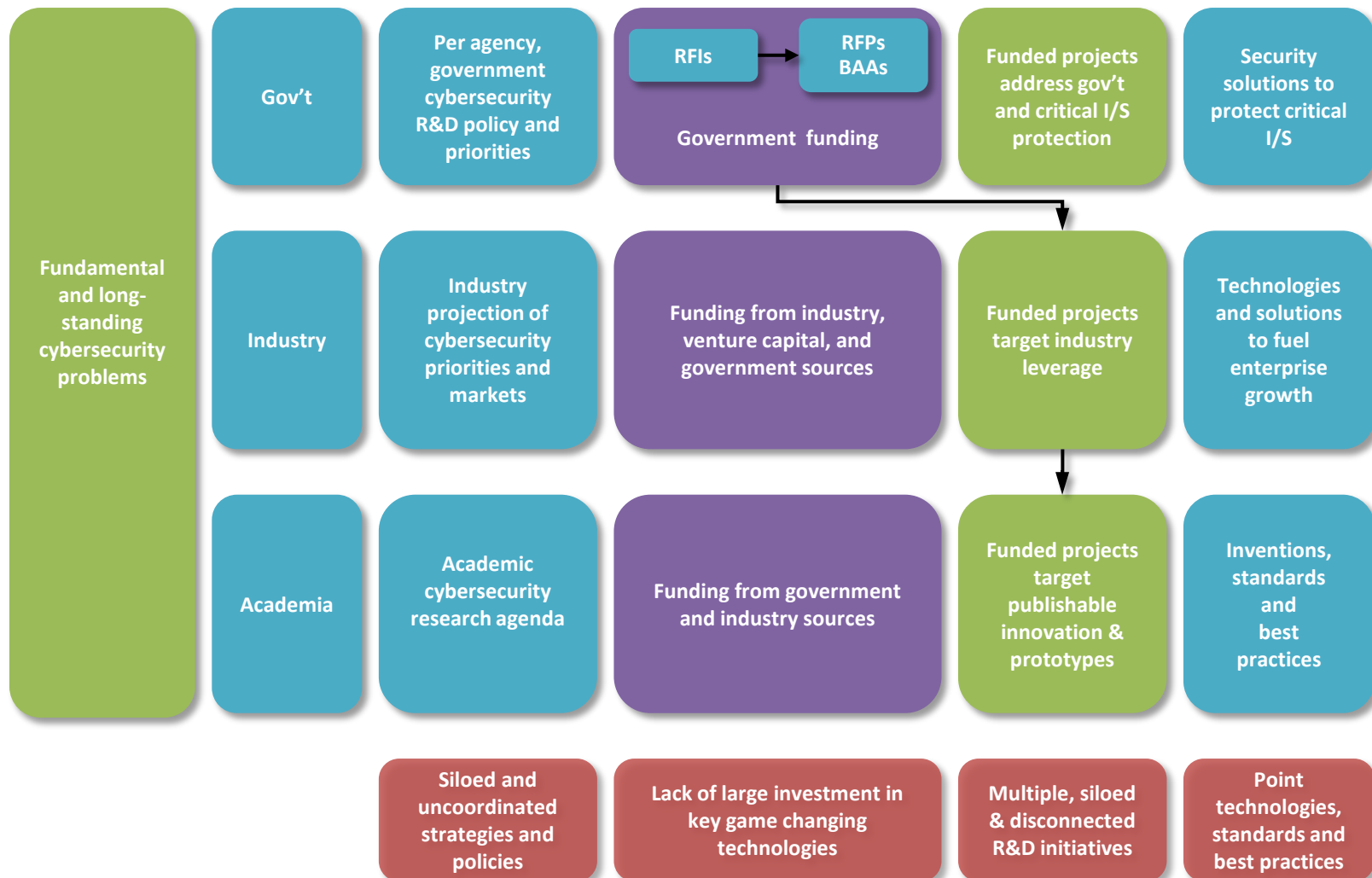
- Corporate research focuses on developing innovations to fuel the organic growth of their enterprises. These innovations are viewed as strategic assets for competing in the marketplace. But industry is not motivated to invest in cybersecurity research and development that does not have near-term tangible economic benefits.



Academia

- Academia primarily engages in long-term basic and applied research in cybersecurity which pushes the frontier of what is known and possible. However, this frontier is often disconnected from the operational reality. Members of this community often find it difficult to move beyond first-level deliverables, such as research papers and limited prototypes.

Industry View of the Landscape



“Opportunity”

Coordinated industry participation to address national cyber security R&D imperatives and create viable game changing solutions

Straw Man Mission for an Industry Led Cyber Security Research Institute

Foster the research and development of game changing solutions to critical cybersecurity challenges through effective government, industry, and academia partnerships

Value Proposition

CSRI will bridge the gap between government funded R&D and commercially available cybersecurity solutions

CSRI will facilitate solutions addressing grand challenges that are bigger than any one company, consortium, sector, or nation

- In-depth problem understanding and definition
- Collaboration on solution implementation

CSRI Key Activities

- Address “grand challenges” in cybersecurity
- Track cybersecurity R&D activities
- Transfer technology

QUESTIONS *for the panel?*