



# Strategic Cyber Risk and Response: Introduction and Context

Sponsored by:

Center for Technology and National Security Policy  
(CTNSP), National Defense University (NDU)



International Cyber Center



# Agenda



- CTNSP
  - Mission, Focus
  - Temporal Perspective
    - Past
    - Present
    - Future
- GMU ICC
  - Mission, Priorities
  - Future
- Closing the Loop



# CTNSP Mission, Focus

- Mission: Explore the nexus between
  - Developments in technology, and
  - National security policy
- Focus
  - Key developments in Information Technology (IT); e.g.,
    - Injection of commercial IT into government systems
    - Cyberspace, cyberpower, cyberstrategy
  - The evolution of Transformation and Complex Operations; e.g.,
    - Humanitarian Assistance/Disaster Relief (e.g., STAR-TIDES)
    - Stability Operations (e.g., Information and Communications Technology)
    - Counterinsurgency, Counter-Terrorism
  - Impact on life sciences (e.g., pandemic influenza)
  - Modeling and Simulation of Human, Social, Cultural Behavior



# Past (1 of 2)

- In response to a request in the 2006 Quadrennial Defense Review, CTNSP has generated two books on cyber issues
- “Cyberpower and National Security Policy” (Potomac Press)
  - Foundation (lexicon, theory, policy)
  - Cyberspace (trends, issues)
  - Cyberpower (impact of cyberspace on military, information levers of power)
  - Cyberstrategy (impact of cyberspace on terrorists, criminals, near-peers, deterrence)
  - Institutional Factors (governance, legal, organizational)
- “Military Cyberpower” (CTNSP, NDU)
  - Context and overview
  - Perspectives from representatives from the Services



## Past (2 of 2)

- What – Workshop on Cyber Deterrence
- Who -- Sponsor: OUSD(Policy); Chair: Terry Pudas, CTNSP
- When, Where -- October 20 – 21, 2008; NDU
- How – Eight panels; e.g.
  - Theory of Deterrence
  - Challenges in a New Global Commons
  - Thresholds and Response
  - The New Article V
  - How to Invest?
  - Ambiguity vs Explicit Declaration
  - Critical Infrastructure
  - How to Move Forward?



# Present



- “Strategic Cyber Risk and Response” Seminar
  - Focus:
    - “What cyber advice would you offer to the new Administration?”
    - “How would you strengthen/build Communities of Interest coming out of the seminar to drive progress in creating and implementing national strategic cyber priorities?”
  - Structure
    - “Attacks, Preparedness, and Response”
    - “Cyber Risk”
    - “Malicious Activity and Cybercrime”
    - “R&D Requirements Planning”
    - “Governance of Cyber”
- Paper: “The Challenges in Assessing Cyber Issues”



# CSIS: Major Findings



- Cybersecurity is now a major national security problem for the US
- Decisions and actions must respect privacy and civil liberties
- Only a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure



# Future: CTNSP

- CTNSP is planning to convene several cyber conferences/workshops
  - “International Cyber Perspectives” (Spring)
  - “Harmonizing Civil Liberties and National Security” (Summer)
  - “Sizing the Cyber Force” (TBD)



# Agenda



- CTNSP
  - Mission, Focus
  - Temporal Perspective
    - Past
    - Present
    - Future



## GMU ICC

- Mission, Priorities
- Future
- Closing the Loop



# International Cyber Center (ICC)



- Mission: facilitate strategic collaboration and information sharing to better identify and address global cyber issues
- Priorities:
  - Capacity: Promote IT proliferation/CERT capacity building in the developing world
  - Risk: Develop collaboration framework to assess and mitigate risk to global ICT
  - Response: Enhance global ICT preparedness – situational awareness, analysis, information sharing, response, and recovery
  - Crime: Strengthen coordinated, global effort against malicious activity and cyber crime to reduce frequency, impact, and risk
  - R&D: Enhance global coordination to better assess and mitigate risk, and address long-term hard problems in cyberspace



# Future: International Cyber Center of GMU



- ICANN/Georgia Tech/ICC DNS workshop (at GA Tech) (Feb 3-4, 2009)
- Envisioned Initiatives
  - International Cyber Initiatives
  - CERT capacity building in emerging countries
  - International Watch and Warning Network
  - Oxford University Summer Program – Global Issues and Cyber Security
  - Follow up to March 08 GMU R&D symposium in Europe
  - DNS Security
    - Workshop and Hands-on Training
    - DNSSEC implementation challenges
      - Protects against major DNS weakness
      - SCIT applied to DNSSEC
      - OMB directive to .gov domain users
- Randomized Defense Strategies
  - White paper to AFRL
  - NITRD RFI



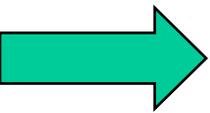


# Agenda



- CTNSP
  - Mission, Focus
  - Temporal Perspective
    - Past
    - Present
    - Future

- GMU ICC
  - Mission, Priorities
  - Future



Closing the Loop



# "Closing the Loop"

- Challenges
  - Our panelists will provide cyber advice to the new Administration -- How can we prioritize that advice?
  - Many participants in the audience are pursuing key cyber initiatives – How can we create and sustain Communities of Interest?
- Proposal – generate a "web-based" survey to elicit
  - Reactions from the audience on proposed advice
    - Employ a Likert scale to rank order the advice
    - Provide feedback to the audience in the form of distributions, mean values
  - Thoughts on creating and sustaining Communities of Interest
- Feedback on the Conference

A URL will be disseminated to provide access to the survey



# Final Observation

“Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it's the only thing that ever does”

– Margaret Mead



# Back-up





# Elements of the Comprehensive National Cybersecurity Initiative (CNCI)



- Move towards managing a single federal enterprise network
- Deploy intrinsic detection systems
- Develop and deploy intrusion prevention tools
- Review and potentially redirect research & funding
- Connect current government cyber operations centers
- Develop a government-wide cyber intelligence plan
- Increase the security of classified networks
- Expand cyber education
- Define enduring leap-ahead technologies
- Define enduring deterrent technologies and programs
- Develop multi-pronged approaches to supply chain risk management
- Define the role of cyber security in private sector domains



# Element of Survey



- Add print-out from cyber survey

Context for “Attack, Preparation,  
and Response”:  
Cyber Wargame Highlights

January 22, 2009

# Key Data

- What – Cyber Strategy Inquiry
- Who
  - Sponsors
    - Booz Allen Hamilton
    - Business Executives for National Security (BENS)
  - Participants – 230 from government, industry, civil society
- Where, When
  - Washington, DC
  - December 17 – 18, 2008

# Key Issues

- Privacy versus attribution
- Regulation versus incentives for cybersecurity
- Disclosure versus classification
- Risk management versus resilience

# Key Challenges

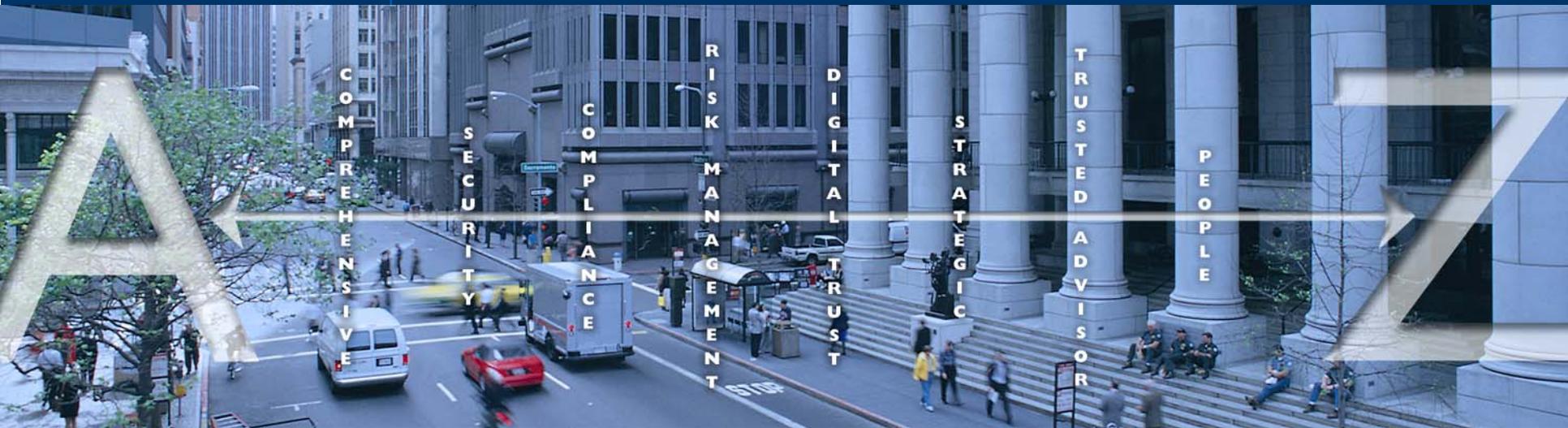
- How to design a legal framework that addresses these issues
- The rules of engagement for a cyberattack
- How to deal with the global aspects of cybersecurity, including the supply chain
- How to educate and train the next generation

# Key Take-Aways

- Mark Gerencser, BAH
  - Leadership
    - “There really wasn’t anyone in charge of all of cybersecurity”
    - “... perhaps there can’t be one person or entity in charge,”
    - “so cybersecurity requires distributed leadership”
  - Interdependencies
    - “...there were interdependencies that we didn’t quite understand or appreciate before”
- Rep. James Langevin (D-R.I.)
  - “The cyberthreat itself is ever changing and ever evolving,...”
  - “It is going to be very difficult to stay one step ahead of it,...”
  - “We’re way behind where we need to be now”

# Cyber Preparedness & Response - Advice for a New Administration

“Strategic Cyber Risk and Response” Conference,  
National Defense University’s Center for Technology and  
National Security Policy and George Mason University’s  
International Cyber Center, 22 January 2009, Fort McNair



Guy Copeland, Vice President  
Information Infrastructure Advisory Programs and  
Special Assistant to the CEO, CSC





# President Obama's Agenda to Protect our Information Networks

- ***Strengthen Federal Leadership on Cyber Security***
- ***Initiate a Safe Computing R&D Effort and Harden our Nation's Cyber Infrastructure***
- ***Protect the IT Infrastructure That Keeps America's Economy Safe***
- ***Prevent Corporate Cyber-Espionage***
- ***Develop a Cyber Crime Strategy to Minimize the Opportunities for Criminal Profit***
- ***Mandate Standards for Securing Personal Data and Require Companies to Disclose Personal Information Data Breaches***



# Testimony of Department of Homeland Security Secretary Designate, Janet Napolitano

**“The federal government cannot do this alone. ...we will provide more effective means for the private sector to join us in meeting our goals for the safety and security of our nation.”**

<http://hsgac.senate.gov/public/files/011509Napolitano.pdf>



# Government and Private Sector Efforts

- ***a large number of professional membership organizations, associations, government bodies and treaty organizations that are active (ITU, IETF, FIRST, ISSA, SANS, NANOG, ISA, ITAA, etc);***
- ***Under the National Partnership Model for Critical Infrastructure Protection sectors have formed Sector coordinating Councils;***
- ***The Partnership for Critical Infrastructure Security (PCIS) and the Department of Homeland Security have organized the Cross Sector Cyber Security Working Group (CSCSWG) made up of over 90 representatives from all the Sector Coordinating Councils and their counterpart Government Coordinating Councils;***
- ***The Information Technology Information Sharing and Analysis Center (IT-ISAC) is collaborating across most of the 17 sectors and, in particular, is working with the National Coordinating Center for Telecommunications (NCC) and the United States Computer Emergency Response Team (US-CERT) ;***
- ***And many, many more***



# Information Technology Sector Accomplishments



- ***Development of a sector-wide risk assessment;***
- ***Integrated planning and execution of major cyber exercises (e.g. Cyber Storm I and II);***
- ***Improved operational integration in times of national emergency (e.g., hurricanes);***
- ***Development of the IT Sector-Specific Plan; and,***
- ***Cross sector planning and interaction through the Partnership for Critical Infrastructure Security (PCIS) and the Cross Sector Cyber Security Working Group.***



# Information Technology Sector Priorities for Urgent Attention



- ***Elevation of cyber security to a senior White House policy advisor and office with adequate staffing and resources;***
- ***Less focus on planning and more concentration on action;***
- ***More transparency with private industry in the execution of the Comprehensive National Cyber Initiative (CNCI);***
- ***Integrate the operational capabilities of the US Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center for Telecommunications (NCC), to include private sector subject matter expert participation;***
- ***Establish clear mechanisms between government and industry for improved situational awareness and response;***
- ***Fully integrate the private sector critical infrastructure community into the planning and execution of efforts to protect the nation's critical infrastructure; and,***
- ***Define a clear strategy for international cyber security engagement.***



# Some Specific Suggestions

- **For immediate improvement of our operational preparation and responsiveness, create a government funded, National Crisis Coordination Center**
  - **2004 Recommendation of the Early Warning Task Force of the National Cyber Security Summit**
  - **Later recommended by the President's National Security Telecommunications Advisory Committee (NSTAC) in a report on Next generation Networks and being examined again now**
  - **Also, recent Center for Cyber Security Operations described in report of the CSIS Commission on Cybersecurity for the 44<sup>th</sup> Presidency**
  - **House government, industry and academic security experts, both physical and cyber.**
  - **Jointly prepare, exercise, evaluate and update National Joint Crisis Response plans to prevent, detect and respond, Conduct joint exercises at the national level to train and test the plans**
  - **Governance, including mandatory ethical rules, must be established and documented for all participants, based on true partnership principles**
  - **Congressional Charter**



## Some Specific Suggestions - 2

- **Make better use of tools and organizations in place**
  - **Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) should be pushed to all eligible users**
  - **Increase use of Telecommunications Service Priority (TSP)**
  - **Sector Information Sharing and Analysis Centers**  
The IT ISAC plays a lead cross-sector role for cyber
  - **Fully Integrate private sector, state, local, tribal and key international into planning, operations and exercises at every phase as full and equal partners**
  - **Apply true partnership principles, and do not simply invoke rules and regulations derived from acquisition and regulatory relationships, even if a legislative waiver or exception is required.**
- **Make US representation to relevant international standards bodies more robust**





## Some Specific Suggestions - 3

- **Provide an authoritative structure for codifying, evolving and using informed expert judgment to apply known standards, practices and other criteria for cyber security**
  - **Information Systems Security Board (ISSB) was a recommendation of the President's National Security Telecommunications Advisory Committee**
  - **Need for such an organization was identified by the National Research Council (NRC) as early as 1991**
  - **Evaluate and endorse information systems security standards and practices and evaluation/testing criteria.**
  - **Develop and maintain information systems security principles (ISSP).**
  - **Develop rating criteria to identify varying levels of security.**
  - **License testing laboratories and auditing organizations**
  - **Congressional Charter**



THE UNITED STATES  
CYBER CONSEQUENCES UNIT

# Recommendations for NDU Cyber Risk and Response Conference

January 2009

Scott Borg

Director and Chief Economist  
U.S. Cyber Consequences Unit

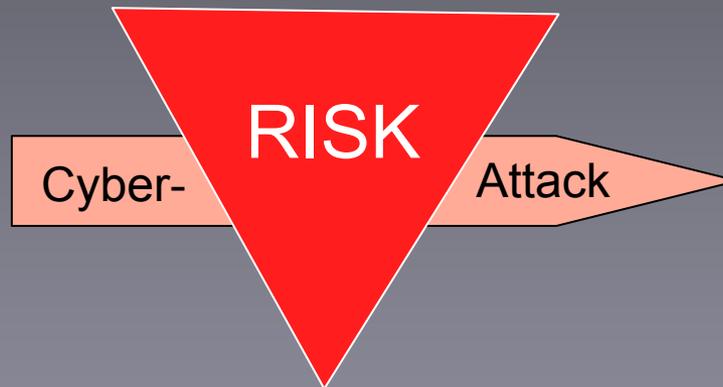


Risk (annualized expected loss) from cyber is being allowed to build up without being charged as a cost, because most of it hasn't had to be paid out yet. This is what we did with mortgages. But the cyber risks are much worse.

## RISK COMPONENTS

Threats

Consequences



Vulnerabilities

$$\text{RISK} = \text{THREATS} \times \text{CONSEQUENCES} \times \text{VULNERABILITIES}$$



The sheer scale of economic damage that could be done by cyber-attacks on critical infrastructure industries is not being taken seriously enough . . .

<b>Critical Infrastructure Industry</b>	<b>Direct Percent of GDP</b>	<b>Effective Percent of GDP</b>	<b>Dependent Percent of GDP</b>
Electric Power	1.5	3.4	<b>72</b>
Oil and Gas Fuel	1.0	3.0	<b>71</b>
Telecom & Internet	2.6	4.9	<b>62</b>
Banking and Finance	5.7	8.6	<b>59</b>
Water and Sanitation	< 1	< 1	<b>40</b>
Chemical Industries	1.7	4.1	<b>33</b>
Air Transport	0.5	2.0	<b>24</b>
Ground Transport	2.1	4.0	<b>62*</b>
Health Care	6.7	15.4	<b>16</b>

One much needed policy response →



## Develop a **National Cyber-Recovery Plan** for Large-Scale Attacks on Critical Infrastructure Industries

- Analogous to the nuclear civil defense plans
- An ongoing project to be conducted by a small, task oriented organization
- Extensive industry involvement at each stage
- Describing successive phases of action, including measures to provide essential supplies and restore trust
- Accompanied by a mandate for distributing and exercising significant portions of the plan
- Making the nature of the problems clear to industry and the public, including the possible re-engineering measures to reduce consequences



Many cyber-security trade-offs are not being sufficiently analyzed, such as the plans for stopping government information leakage . . .

CONDITIONS CONDUCTIVE TO LARGE-SCALE, HIGH-CONSEQUENCE CYBER-ATTACKS	
FACTORS INCREASING SCALABILITY OF ATTACKS	FACTORS DECREASING SCALABILITY OF ATTACKS
I. Uniformity of Targets	I. Diversity of Targets
II. Centralization of Targets	II. Decentralization of Targets
III. Common Access Route	III. No Common Access Route
IV. Higher Level of Automation	IV. Lower Level of Automation
V. Regularity of Labeling Conventions	V. Irregularity of Labeling Conventions

One much needed policy response →



## Create a **National Cyber Policy Board** to Review and Direct National Cyber-Security Measures

- An ongoing think tank of nationally recognized cyber-security experts who have a broad understanding of the economic and strategic dimensions of the field
- Working closely with a Deputy National Security Advisor for Cyber Security
- Outside of the old nuclear planning agencies and existing federally funded research and development centers
- Maintaining strong, but highly selective channels to and from academic departments
- Providing industry with an expert group midway between the government and the private sector with whom they can have high level, but actionable discussions



Many economic drivers affecting cyber-security are not being sufficiently utilized . . .

**THE SIX BASIC REASONS FOR “MARKET FAILURES”**  
(BORG SYNTHESIS)

1) Companies not being charged for all their inputs or not being paid for all their outputs

2) Individual agents acting on behalf of companies are not adequately motivated to act in the long term interests of their company

**3) Lack of information for comparative market choices**

4) Absence of model products, first suppliers, or first customers needed to “seed” a market

5) Excessive switching costs, often caused by a) government regulation or b) lock-in enforced by patents or copyrights (another kind of government regulation)

6) Entry barriers, causing a lack of competing alternatives

One much needed policy response →



## Establish a **Cyber-Security Rating Agency** to Evaluate the Security of Commercial Over-the-Counter Software

- Analogous to automobile crash ratings, energy efficiency ratings, and nutritional ratings
- Resulting in a simple, numerical scale, easy for consumers to understand
- Relying on automated tests that would evolve and be constantly improved over time
- Getting rated would be voluntary, but unrated software would be labeled “security unrated”
- Acknowledged to be highly imperfect, but still useful as a broad indicator
- Implement gradually or in phases, so that the market consequences can be gauged and adjusted



Thank you!

For more information or permission to use this material,  
please contact:

Scott Borg  
U.S. Cyber Consequences Unit  
P.O. Box 1390  
Norwich, VT 05055



# Managing Cyber Risk

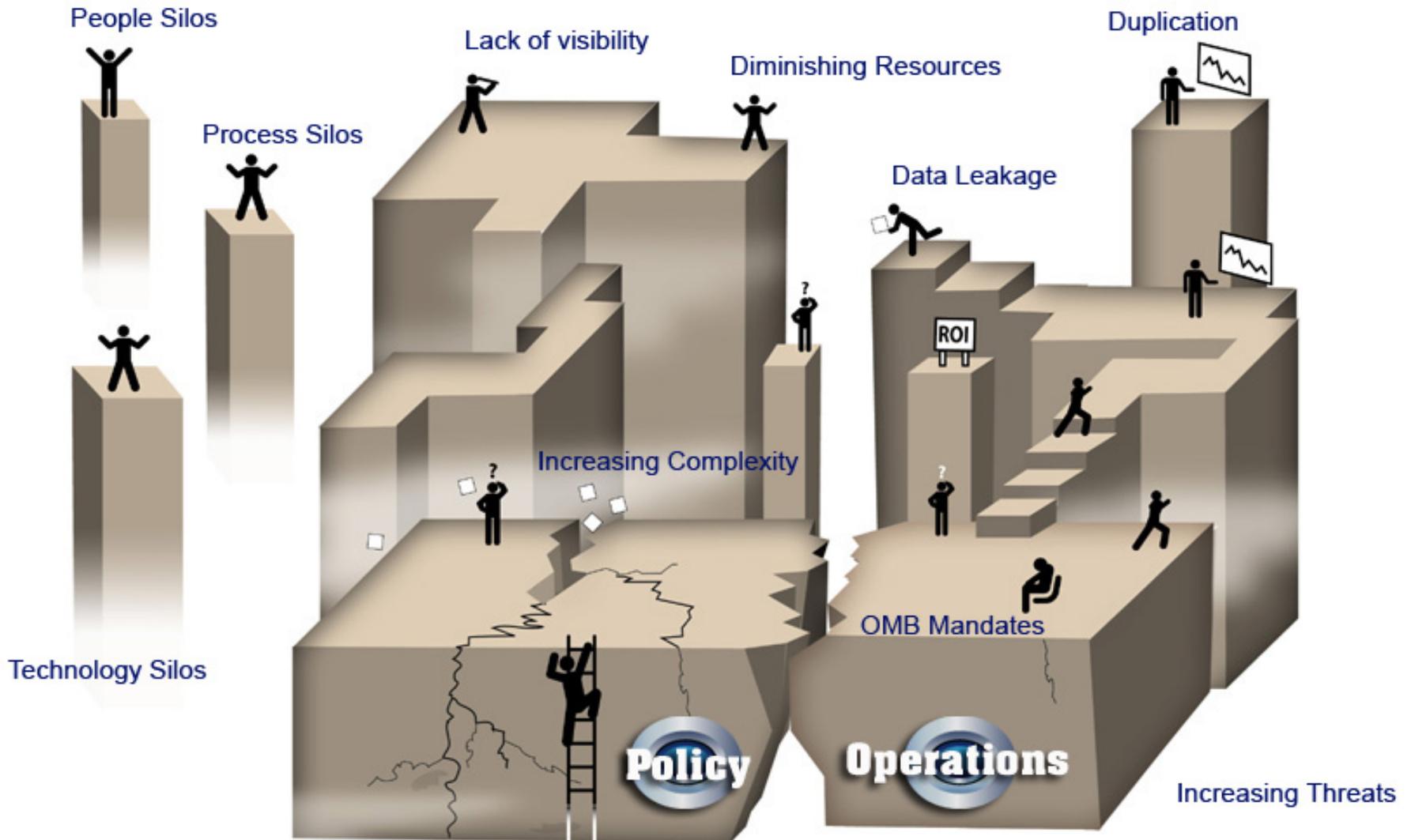
*Balancing Risk and  
Preventing Cyber Attacks*



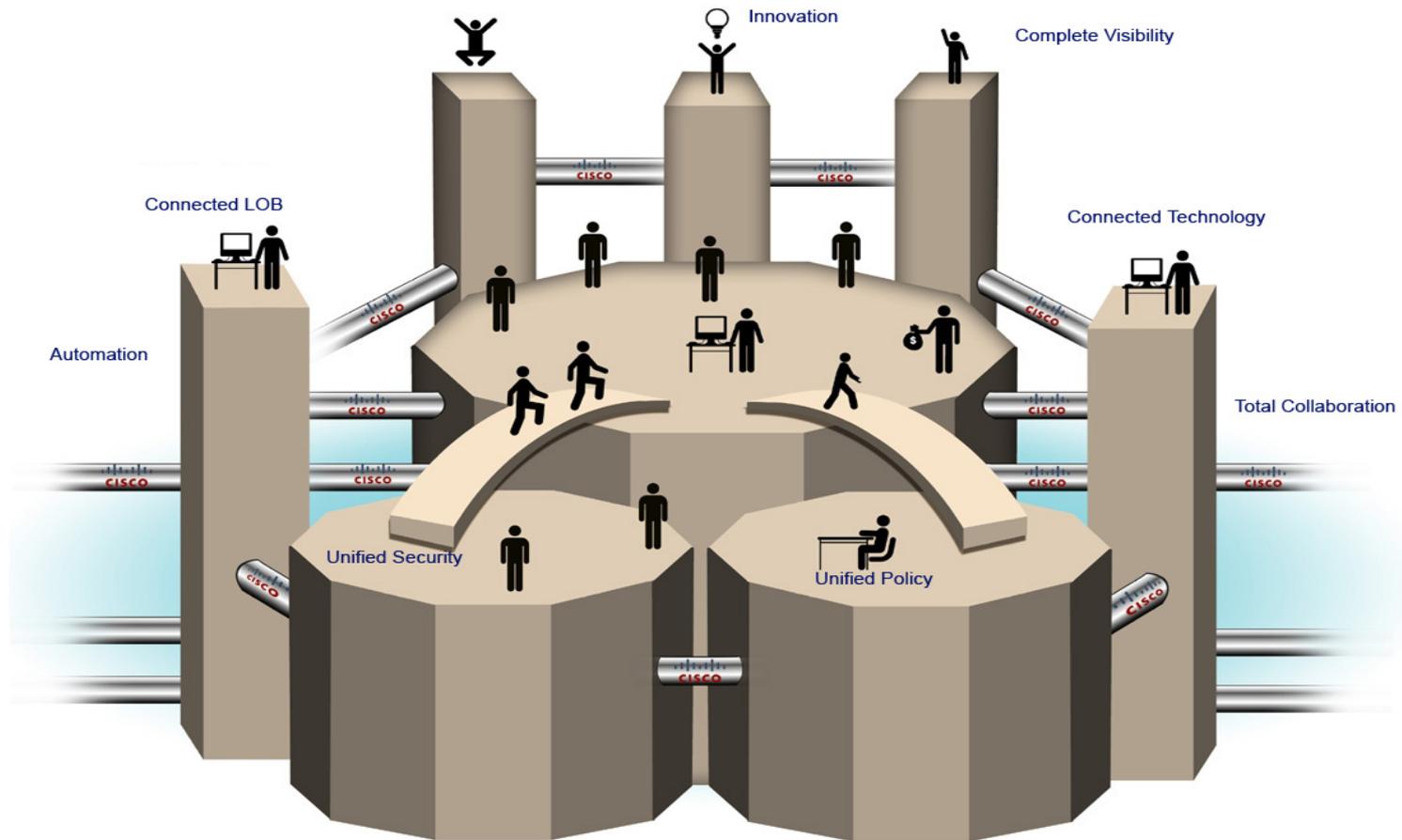
**David Graziano, Federal Security Solutions**

**January 22, 2009**

# Fragmentation = Risk



# Leverage Existing Infrastructure





Best Practice: Policy Enforcement

**Create compartmentalization**

Reduce network “flatness”

## Best Practice: Email Security

**Encourage grass-roots DNS registration  
of outbound email IP addresses**

**Fight SPAM**

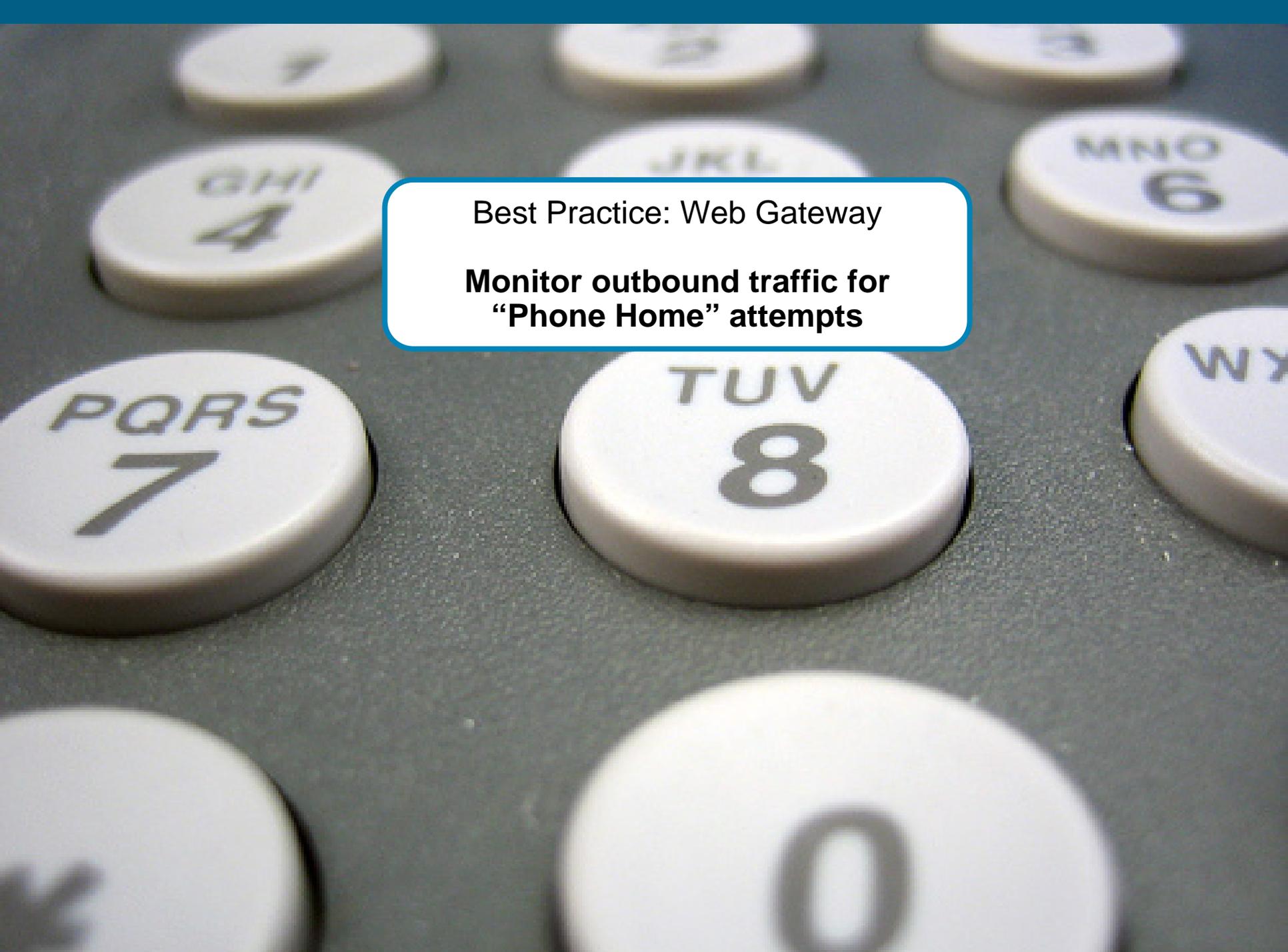




Best Practice: Email

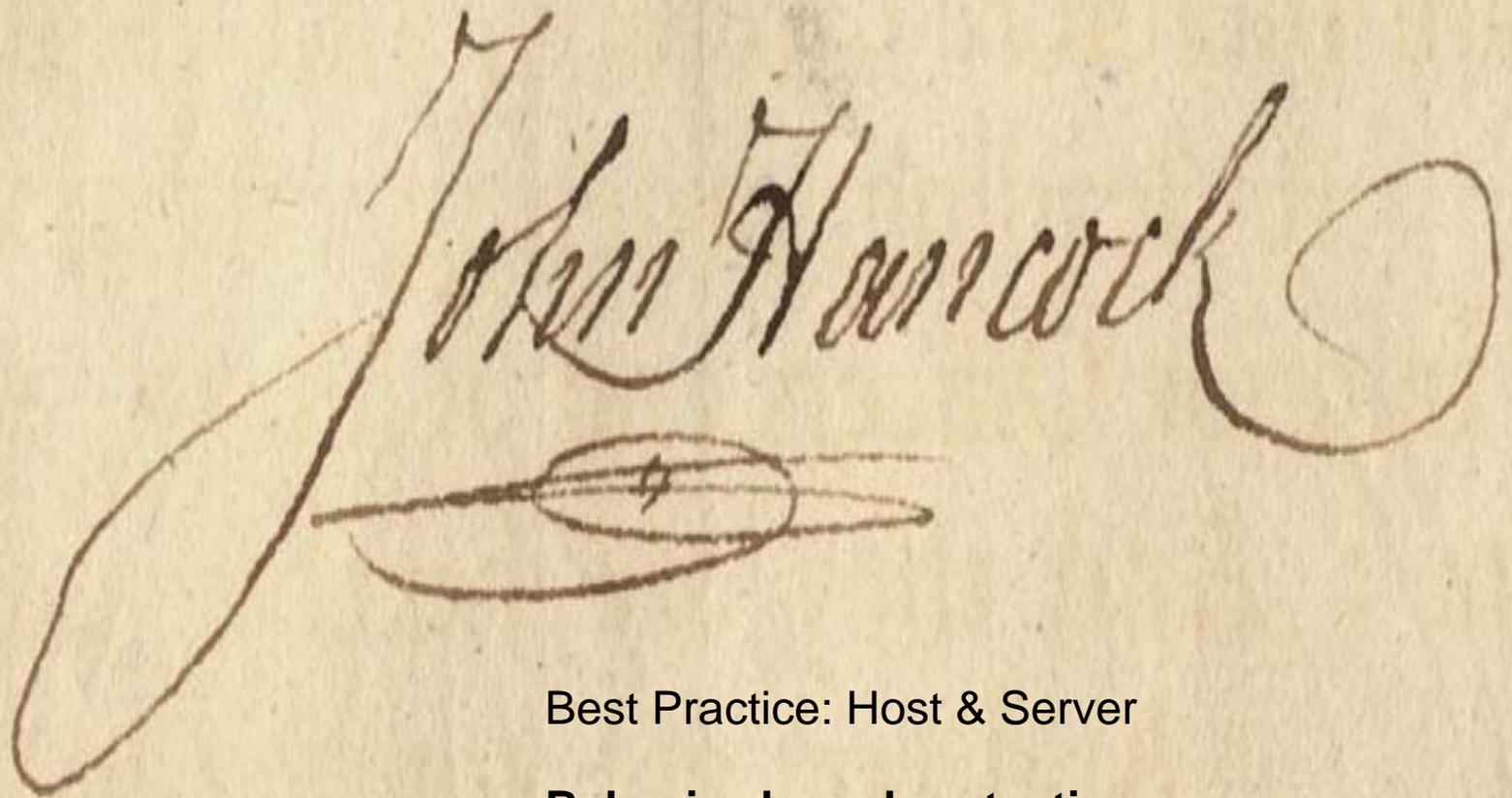
**Reputation-based Filtering**

Improve accuracy

A close-up photograph of a telephone keypad. The keys are white with black text. A semi-transparent white text box with a blue border is centered over the keypad. The text box contains the text: "Best Practice: Web Gateway" and "Monitor outbound traffic for 'Phone Home' attempts". The keypad keys visible include "7 PQRS", "8 TUV", "9 WXYZ", "4 GHI", "5 JKL", "6 MNO", and "0".

Best Practice: Web Gateway

**Monitor outbound traffic for  
"Phone Home" attempts**

A handwritten signature in brown ink on aged, yellowish paper. The signature reads "John Hancock" in a highly stylized, cursive script. The letter "J" is particularly large and loops around the rest of the name. The paper shows signs of age, including a small tear at the top center and some faint smudges.

Best Practice: Host & Server

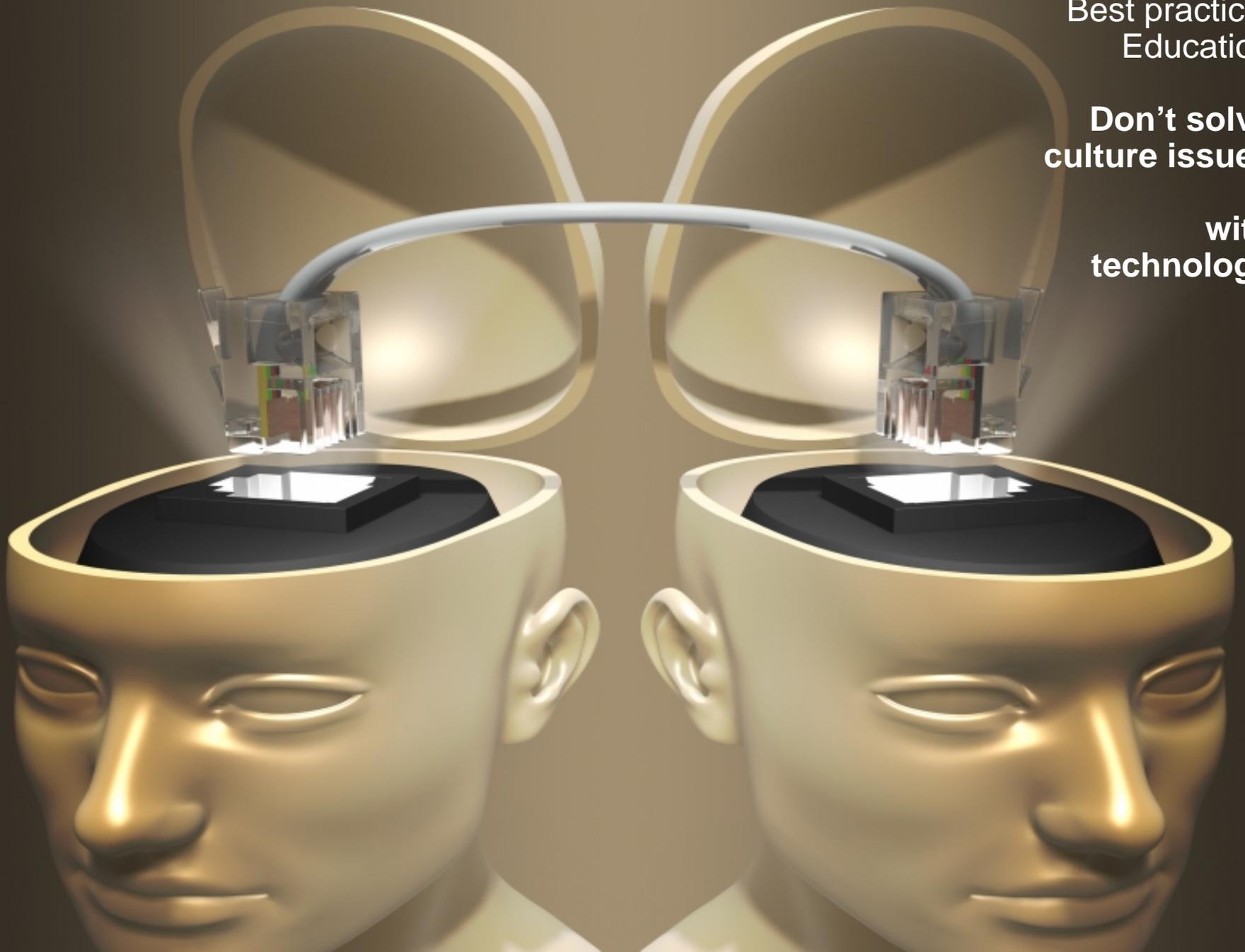
**Behavior-based protection**

Not based on signatures

Best practice:  
Education

**Don't solve  
culture issues**

**with  
technology**



Comprehensive Security Awareness...  
**Don't boil the ocean.**



# Our Invitation



# New Cisco Security Center

The screenshot shows the Cisco Security Center website. At the top, there is a navigation bar with the Cisco logo, a search bar, and links for 'Log In', 'Register', and 'About Cisco'. Below the navigation bar, there are tabs for 'Solutions', 'Products & Services', 'Ordering', 'Support', 'Training & Events', and 'Partner Central'. The main content area is titled 'Cisco Security Center' and features a section for 'Inform, Protect, Respond' with a sub-header 'Powered by IntelliShield'. This section contains a table of security alerts with columns for 'Security Alerts', 'CVSS Score', 'Cisco IPS Signature', 'Cisco PSIRT Advisory', 'Cisco IntelliShield Mitigation Report', and 'Known Cisco Products Affected'. The table lists several vulnerabilities, including Microsoft Exchange IMAP Literal Processing Denial of Service Vulnerability, Cisco IOS SSL ClientHello Message Denial of Service Vulnerability, F5 FirePass 4100 VPN my.activation.php3 Arbitrary Code Execution Vulnerability, Symantec Storage Foundation for Windows Scheduler Service Authentication Bypass Vulnerability, and Mozilla Firefox SeaMonkey and Thunderbird JavaScript Engine Memory Corruption Vulnerability. To the right of the table, there is a 'Cisco Emergency Response' section with links for urgent assistance, reporting incidents, and contacting the Cisco TAC. Below the table, there is a 'Track and Analyze' section with a map showing threat activity sources and virus outbreak levels across different regions. To the right of the map, there is an 'Improve Your Security' section with a video player and a 'Learn More' link. At the bottom, there are links for 'Additional Resources' such as 'Design Zone for Security', 'Resources for Chief Security Officers', 'IntelliShield Mitigation Reports', 'Remote Worker Security', 'Security Podcasts', 'White Papers', and 'Case Studies'. There is also a 'Product and Service Updates' section with links to subscribe to various alerts and services.

Security Alerts	CVSS Score	Cisco IPS Signature	Cisco PSIRT Advisory	Cisco IntelliShield Mitigation Report	Known Cisco Products Affected
<a href="#">Microsoft Exchange IMAP Literal Processing Denial of Service Vulnerability</a>	3.3/2.4				
<a href="#">Cisco IOS SSL ClientHello Message Denial of Service Vulnerability</a>	3.3/2.7				
<a href="#">F5 FirePass 4100 VPN my.activation.php3 Arbitrary Code Execution Vulnerability</a>	10.0/7.4 <b>HOT</b>				
<a href="#">Symantec Storage Foundation for Windows Scheduler Service Authentication Bypass Vulnerability</a>	2.3/1.7				
<a href="#">Mozilla Firefox SeaMonkey and Thunderbird JavaScript Engine Memory Corruption Vulnerability</a>	8.0/5.9				

**NETWORKWORLD** 20 Most Useful IT Security Websites

Vendor-neutral security threat intelligence

Expert mitigation techniques

Current trend analysis:  
IntelliShield Cyber Risk Report

Real-time threat-activity mapping

[www.cisco.com/security](http://www.cisco.com/security)

# Cisco Security IntelliShield Alert Manager Summary



Market leading security intelligence



Reduce costs of patching and remediation



Filtered alerts by your customized profile

**Security Intelligence Services**

For a 6-month trial – see presenter  
[www.cisco.com/go/intellishield/trial](http://www.cisco.com/go/intellishield/trial)

**Cisco Security Center**  
[www.cisco.com/go/security](http://www.cisco.com/go/security)

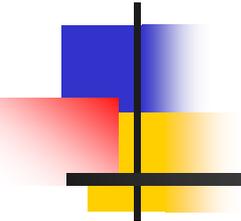


# For Today's Attendees: Free 6 Months

- Free six-month subscription to IntelliShield
  - See David Graziano, Cisco – after the presentation
-



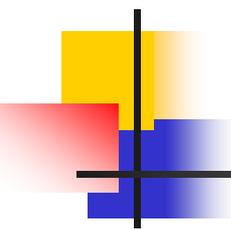
**CISCO**



# Cyber Security R&D – what's next?

---

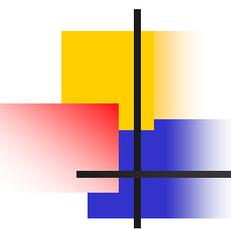
Annabelle Lee  
Senior Cyber Security Strategist  
Computer Security Division  
January 2009



# Presentation Overview

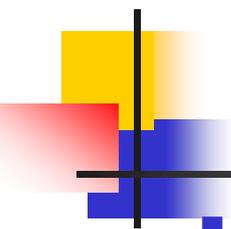
---

- NIST R&D Responsibilities
- Information Technology Laboratory (ITL)
- Current Cyber Environment
- Computer Security Division (CSD) agenda...



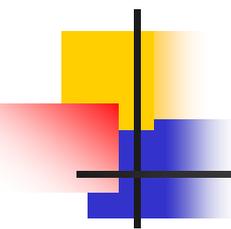
---

# NIST R&D Responsibilities



# NIST R&D Responsibilities

- Under FISMA NIST shall “*conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security.*”
- In accordance with the Cyber Security Research and Development Act, NIST *develops, and revises as necessary, checklists setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government*
- Homeland Security Presidential Directive (HSPD) 7; “*The Department of Commerce will work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts...*”



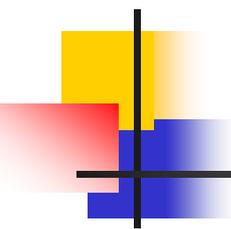
---

# Information Technology Laboratory (ITL)

# Community Engagement

## Representative Customers and Collaborators

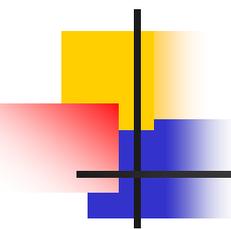




# Community Engagement

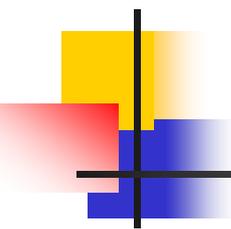
---

- Industry
  - Accessing Expertise and Leveraging Resources
  - Coordinating Standards and Initiatives
- Academia
  - Accessing Expertise and Leveraging Resources
  - Representative Institutions and Consortia
- International
  - Formal Standards Groups
  - Accessing Expertise and Leveraging Resources
- Federal, State, and Local Government
  - Interdepartmental
  - Department of Commerce
  - State and Local Governments



---

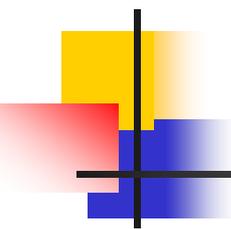
# Current Cyber Environment...



# Current Environment: Attackers

---

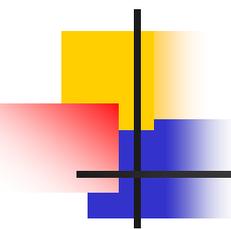
- Currently, there are significant advantages for an attacker:
  - Increased dependence of our society on interconnected systems
  - Required resources (funding, equipment, and training) are readily available
  - Powerful attack tools are now available over the Internet to anyone who wants them
    - Little skill or sophistication is required to initiate extremely harmful attacks



# Current Environment: Attackers (2)

---

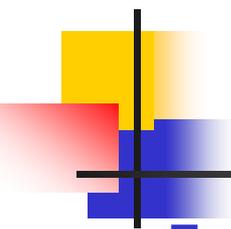
- Result: The sophistication of the attack is growing
- Also, the sophistication of the attackers is increasing
- The gap between an attackers' ability to attack and the defenders' ability to defend is widening



# Current Environment: Threat and Vulnerability Trends

---

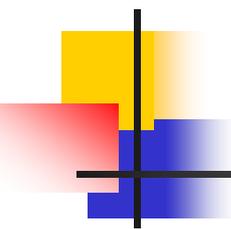
- The rate of development and deployment of malicious code has significantly increased. Underlying operating systems continue to contain undetected bugs.
- Because of the rate of technology change, development of new cyber security technology lags behind deployment of malicious code/technology
- Insiders continue to compromise sensitive information and information systems



# Current Environment: Technology Trends

---

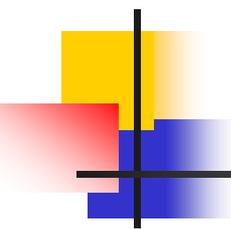
- Convergence in the telecommunications sector is eliminating the distinction between voice and data communications
  - Critical communications become vulnerable to Internet threats
- Interconnectivity is increasing and will continue to increase
  - Outward facing networks are integrated with internal business networks, and with networks supporting critical infrastructures/operations
- The need for cyber security underlies all critical infrastructures that rely on information technology



# Current Environment: Status...

---

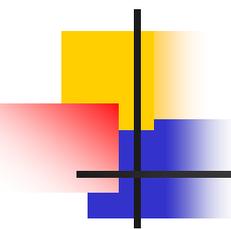
- Because of the availability and pervasive use of the Internet
  - Attack detection and response continues to play “catch up”
  - Federal government is frequently in *reaction* mode
    - Solutions may be costly



# CSD Cyber R&D Agenda

---

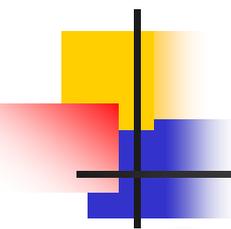
- Provide continuity of government to ensure security of
  - The government's cyber infrastructure and
  - The assets required for supporting essential missions
- Allocation of resources for R&D must be driven by
  - Imminent threat and known intent and
  - R&D planning must anticipate trends and expectations for the next 3 years, 5 years, 10 years...



# CSD R&D Activities

---

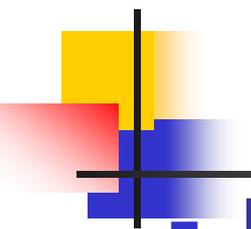
- Current CSD R&D paradigm
  - Incremental improvements
    - Focus on near-term objectives
  - Two to five year time frame
  - Longer term R&D



# CSD Cyber R&D Activities

---

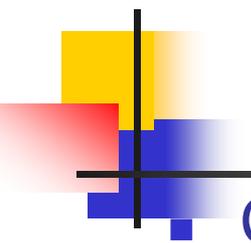
- Reducing the threat space
  - National Vulnerability Database (NVD)
    - U.S. government repository of standards based vulnerability management data
    - Over 60 million hits per year
    - Second only to the NIST atomic clock in accesses
    - Required by the credit card industry (private sector)
  - Security Content Automation Protocol (SCAP)
    - Enables automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance)
    - Federal Desktop Core Configuration (FDCC)
  - Combinatorial testing



# CSD Cyber R&D Activities (2)

---

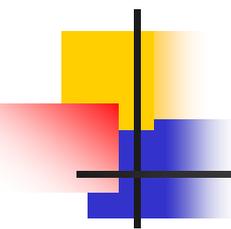
- Product assurance
  - Integrating SCAP settings into configuration settings, e.g., FDCC and SP 800-53, *Recommended Security Controls for Federal Information Systems*
  - Automated assessment of SP 800-53 and SP 800-53A (*Guide for Assessing the Security Controls in Federal Information Systems*)
- Supply chain risk management (SCRM)
  - Key practices guide for the federal government
- Voting
  - Security tests for voting systems
  - Overseas voting



# CSD Cyber R&D Activities (3)

## ■ Cryptography

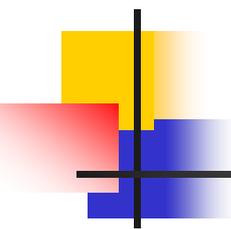
- New hash algorithm (SHA-3) competition
  - Response to recent advances in the cryptanalysis of hash functions.
  - To be used for digital signatures, message authentication and other applications.
- Key management
  - PIV cards – card management and physical access control
  - Key management for wireless
- Random number generator (RNG) standards
  - Entropy sources
- FIPS 140-3, *Security Requirements for Cryptographic Modules*
  - Side channel attacks, e.g., simple power analysis (SPA) and differential power analysis (DPA)
- Quantum resistant public key cryptography
- Cryptanalysis



# CSD Cyber R&D Activities (4)

---

- Emergent technologies
  - Virtualization in cloud computing
    - Application of security
- Access control and privilege management – policy machine
  - Address multiple authentications
  - Address access control at the process level
  - Advanced models



# Questions??

---

Annabelle Lee

Senior Cyber Security Strategist

NIST

100 Bureau Drive, Stop 8930

Gaithersburg, MD 20899-8930



# From Cyber to Information Power: Governing It

Dr. Dan Kuehl

Information Resources Management College (IRMC)

National Defense University (NDU)

Ft McNair Washington, D.C.

**My Opinions:** not the USG, DOD, or NDU!





# Information Power



- “Combination of information content and technology used as a strategic instrument to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security strategies & objectives”
  - Drs Dan Kuehl/Bob Neilson, Georgetown’s *NSSQ* 1999
  - President Ronald Reagan: NSDD 130 (1984), National Security Strategy (1987)
- “The relative ability to **operate in and exploit the information environment** — the aggregated and synergistic combination of **CONNECTIVITY, CONTENT, & COGNITION**. It is employed across all other forms of human activity— economics, war, diplomacy— and across all levels of conflict, from peace to war. Its elements can be described, and its impact measured, albeit not necessarily to the exactness as other components of power.”
  - Dan Kuehl, “The Information Revolution & the Transformation of Warfare” (2007)



# Information Environment

- **Physical/Electronic Connectivity: “Ether”/Cyberspace/”eSpace”**
  - Infrastructures, wires, networks, etc: a means of delivery
  - A unique domain (land, sea, air, space)
  - Includes human non-technical connectivity
- **Information Content:**
  - Words, images, databases, 11010111000s
  - Deeds are content
- **Cognitive: “influence/perception”**
  - **Meaning and the Mind**: “most important”
    - Example: Serbian TV vs NATO’s political cohesion 1999
  - Losing the battle here may negate winning kinetically
  - Al Q’aida using kinetic ops to create cognitive effects
- **“Theater of Operations – Global Commons”**



# Advice for Obama Admin



- Three Suggestions
  - Do not treat cyberspace in isolation from information environment (See DepSecDef Memo of May 07)
    - Need comprehensive Cyberstrategy as a segment of an even more comprehensive National Info Strategy
  - Grow the Partnership
    - Public Sector: Government (all levels), Military, Congress, Intel, Agencies, etc
    - Private Sector: Industry/Business, Academia, Society
    - International partners and players
  - Build the “3Cs” (next slide)



# Information Strategy: “3Cs”

- Builds on “3Cs”
  - Build, enhance, support **Connectivity**
    - Physical: networks, infrastructures, Information-Communication Technology (ICT)
    - Human: one-one, one-many, many-many (enabled by ICT)
  - Build/Use institutions that create **Content**
    - Get this right and the content will flow
  - Measure **Cognitive** impact
    - USE of Cyber/Info for success (military, economic, diplo, etc)
  - Get the REAL experts (ie. Business-Private Sector)
- All Three require **partnerships** beyond government, military, and especially the private sector to include non-US, and they require a long-term view...this isn't years, it's decades
  - Taliban: “Americans have the watches, we have the time”



# President Obama & Cyber



## *Protect Our Information Networks*

Barack Obama and Joe Biden -- working with private industry, the research community and our citizens -- will lead an effort to build a trustworthy and accountable cyber infrastructure that is resilient, protects America's competitive advantage, and advances our national and homeland security. They will:

**Strengthen Federal Leadership on Cyber Security:** Declare the cyber infrastructure a strategic asset and establish the position of national cyber advisor who will report directly to the president and will be responsible for coordinating federal agency efforts and development of national cyber policy.

**Initiate a Safe Computing R&D Effort and Harden our Nation's Cyber Infrastructure:** Support an initiative to develop next-generation secure computers and networking for national security applications. Work with industry and academia to develop and deploy a new generation of secure hardware and software for our critical cyber infrastructure.

**Protect the IT Infrastructure That Keeps America's Economy Safe:** Work with the private sector to establish tough new standards for cyber security and physical resilience.

**Prevent Corporate Cyber-Espionage:** Work with industry to develop the systems necessary to protect our nation's trade secrets and our research and development. Innovations in software, engineering, pharmaceuticals and other fields are being stolen online from U.S. businesses at an alarming rate.

**Develop a Cyber Crime Strategy to Minimize the Opportunities for Criminal Profit:** Shut down the mechanisms used to transmit criminal profits by shutting down untraceable Internet payment schemes. Initiate a grant and training program to provide federal, state, and local law enforcement agencies the tools they need to detect and prosecute cyber crime.

**Mandate Standards for Securing Personal Data and Require Companies to Disclose Personal Information Data Breaches:** Partner with industry and our citizens to secure personal data stored on government and private systems. Institute a common standard for securing such data across industries and protect the rights of individuals in the information age.

## Defense

**Protect the U.S in Cyberspace:** The Obama-Biden Administration cooperate with our allies and the private sector to identify and protect against emerging cyber-threats.



Dr Dan Kuehl

---



<http://www.ndu.edu/irmc/programs/index.html>

Programs/Certifications for/in...  
Chief Information Officers  
Information Assurance  
Organizational Transformation...



...and **Information Strategists**

# Strategic Cyber Risk and Response

National Defense University  
GMU International Cyber Center

Robert B. Dix, Jr.  
Vice President  
Government Affairs &  
Critical Infrastructure Protection  
Juniper Networks, Inc.

# Strategic Cyber Risk and Response

## Governance of Cyber: Strategic Priorities

- White House Senior Policy Advisor for Cyber Security
- Cyber security infrastructure is part of nation's critical infrastructure- cross sector interdependencies impact national risk profile
- Improved integration of private sector CI/KR community into operational activities- prevention, detection, deterrence, mitigation, response, and recovery, including incident management
- Joint National Preparedness Coordination Center ( JNPCC )
- Coordinated Research & Development
- Global issues- including supply chain risk management

# Strategic Cyber Risk and Response

## Governance of Cyber: Strategic Priorities

Robert B. Dix, Jr.

Vice President

Government Affairs &

Critical Infrastructure Protection