

**Deloitte.**

# Succeeding in a cyber world

## *Federation of Tax Administrators' 26<sup>th</sup> Annual Technology Conference*

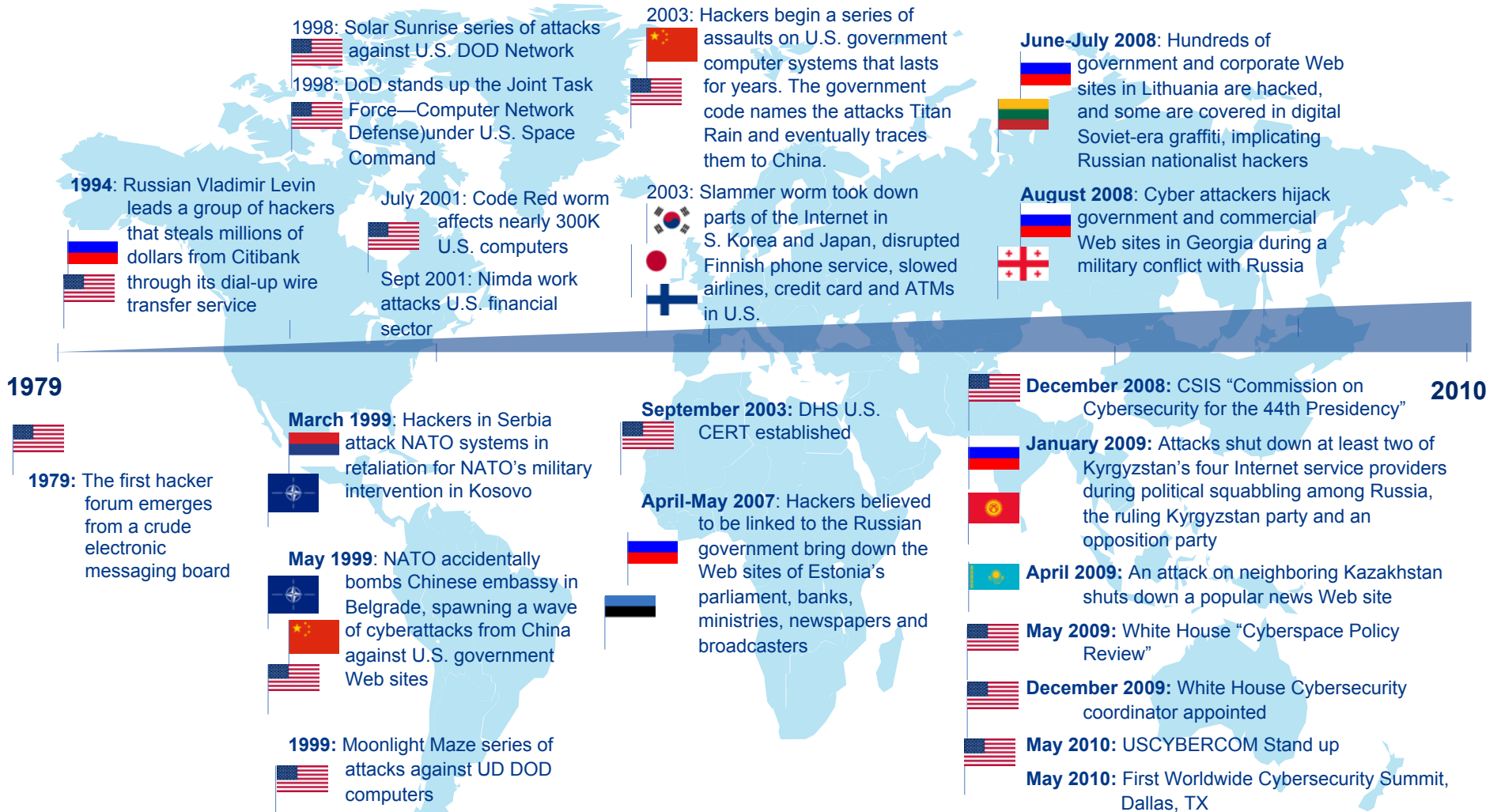
**Harry D. Raduege, Jr.**  
**Lieutenant General, (USAF, Ret)**  
**Chairman, Deloitte Center for Cyber Innovation**

**August 2, 2010**



# State of cybersecurity threats and ongoing challenges

# Cyber threats are borderless...



...U.S. response has been evolving

**By 2013 the Internet  
will be 4X larger than  
in 2009...**



Source: [http://www.calinnovates.org/issues/policy\\_papers/exaflood/](http://www.calinnovates.org/issues/policy_papers/exaflood/)

# The world of cybersecurity

## Threats

- Identity theft
- Information manipulation (e.g. Malware)
- Information theft
- Crime
- Insider
- Espionage
- Cyber attack
- Terrorism

## Targets

- Government (Federal, State and Local)
- Industry
  - Utilities
  - Health care
  - Manufacturing
  - Retail
  - Banking & finance
  - Telecommunications
- Individuals

## Counters

- Cyber workforce
- Network access controls
  - Firewalls
  - Anti-virus S/W
  - S/W patch management
  - ID management
- Dynamic situational awareness
- Risk intelligence & management
- Forensic analysis
- Financial intelligence
- Tighter laws & enforcement ties
- Expanded diplomacy

**You must assume that your network has or will be compromised.**

# Cost to clean up a virus attack: \$6.3 million



**Cost to create a  
virus: -0-  
(hacker tools are free)**



# We've had our cyber wake-up call

## Power Grid is found susceptible to cyber attack

The network of intelligent power switches, called the Smart Grid, could be taken down by a cyber attack. Researchers testing Smart Grid devices for security vulnerabilities have discovered a number of flaws that could allow hackers to access the network and cut power. *ITWorld, 3/21/2009*

"America's failure to protect cyberspace is **one of the most urgent national security priorities.**"

*The Commission on Cybersecurity for the 44th President, The Whitehouse, 6/2009, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*

Federal agencies are facing a severe **shortage of computer specialists**, even during a growing wave of coordinated cyber attacks ...

*Wall Street Journal, 7/22/2009*

Number of **security incidents reported by Federal agencies** to the U.S.-CERT has **dramatically increased** in the past three years, rising from 5,503 incidents in fiscal year 2006 to 16,843 in FY 2008, a 206 percent increase.

*U.S. Government Accountability Office (GAO)*

## Government is vulnerable to cyber attacks

The Federal government is at risk of being unable to fight off attacks on the nation's computer networks unless it strengthens its **cybersecurity work force**. "...our Federal government will be unable to combat these threats without a more coordinated, sustained effort to increase cybersecurity expertise in the Federal work force."

*CNN, Pam Benson 7/22/2009*

[Cyveillance] identified more than 175,000 **distinct phishing attacks** from June through August of this year, "one of the highest three-month volumes ever detected." *Government Computer News, 10/2009*

House leaders called for an "immediate and comprehensive assessment" of Congressional cybersecurity policies, a day after an embarrassing data breach that led to the **disclosure of details of confidential ethics investigations.**

*Washington Post, 10/2009*

In recent months Federal officials have cited the continued efforts of foreign nations and criminals to target government and private sector networks; **terrorist groups have expressed a desire to use cyber attacks** to target the United States; and press accounts have reported attacks on the Web sites of government agencies. *U.S. Government Accountability Office (GAO), 11/2009*

Howard Schmidt appointed White House Cybersecurity Coordinator, **12/22/2009**

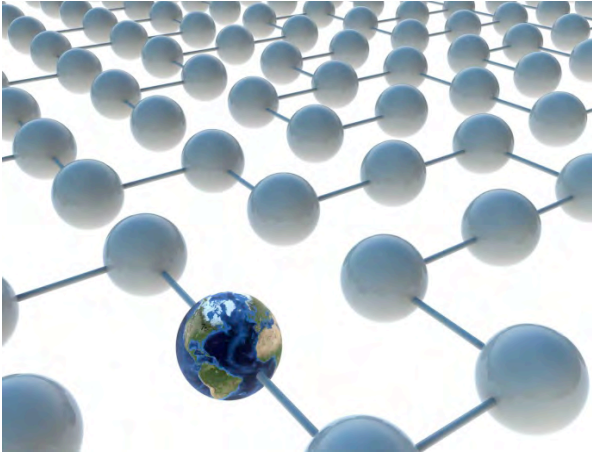
## Web Is New Front Among Cold War Foes

In the new cyber war, the **targets are U.S. companies** as much as embassies or spy services... *Wall Street Journal, 1/14/2010*

The United States stands "... for a **single Internet where all of humanity has equal access to knowledge and ideas.**" *Sec. State Clinton, 1/21/2010*

Hacker Sentenced to 20 Years in Massive Data Theft. *Wall Street Journal, 3/27/10*

Cybersecurity includes all C-levels. *Federal News Radio, April 2010*



**\$1 trillion: 2008**  
**industry estimates of**  
**losses from intellectual**  
**property to data theft**

Source: "Cyberspace Policy Review." The White House, May 2009.

## Ten 2010 cybersecurity protection predictions\*

- Increased vulnerability of mobile devices/smartphones: need to educate users about protection as more applications are provided for smartphones and other mobile devices that facilitate users' ability to do more things related to e-commerce, travel, and business
- Cloud computing: increased adaptation in all sectors — including the public sector — increases need for stronger security
- Increased software testing: needed to reduce the many new vulnerabilities
- Standardizing two-factor authentication: this may become the “norm” in all sectors
- Increased Payment Card Industry (PCI) compliance: drives need for enhanced Web firewalls
- Harm caused by increased number of Network Attached Peripheral Security devices that attach to networks (e.g., unsecured printers and network-connected security cameras), yield more opportunity to cause harm
- Threats to social networking sites: public and private sector face increased vulnerability to sensitive data
- New operating systems: widespread adoption of new operating systems may increase targeted threats
- Increased threats of spam, phishing: some sources indicate rise in threats from China
- Risk of free “fake” antivirus products or scareware: can disable computers and take advantage of computer users and their data

**\*Source: Howard Schmidt, in his capacity as former eBay CISO and vice chairman of the President's Critical Infrastructure Protection Board, *Network World*, 12/21/2009. Note: Howard Schmidt is now the U.S. National Cybersecurity Coordinator.**



**Over 10 million  
Americans are victims  
of identity theft each  
year - and the rate  
grows by more than  
20% annually.**

Source: US DOJ, Office of the Inspector General, "The Department of Justice's Efforts to Combat Identity Theft." March 2010

# Ongoing challenges of designing, implementing, and maintaining a cybersecurity program

Governance/ ownership	Lack of qualified professionals	Expanding digital universe	Unintentional mishandling	Financial implications	Negative impacts
<ul style="list-style-type: none"> <li>• Need for federal, state, local government, and private industry coordination</li> <li>• Need to determine who is responsible for owning and driving cybersecurity activities</li> <li>• States can create new “cybersecurity Director” role, in addition to CISO role</li> </ul>	<ul style="list-style-type: none"> <li>• Federal and state government will be unable to combat cyber threats without a more coordinated, sustained effort to increase cybersecurity expertise in the workforce</li> <li>• “Pipeline” of potential new talent is weak</li> </ul>	<ul style="list-style-type: none"> <li>• Declining cost of computing power, network bandwidth, and storage capacity drive a rapidly expanding digital universe</li> <li>• Worldwide annual data growth rates estimated to increase 58% through 2011 (Source: IDC Forecast of Worldwide Information Growth Through 2011)</li> </ul>	<ul style="list-style-type: none"> <li>• Well-intentioned employees simply getting their jobs done may inadvertently put information at risk, sometimes resulting in data leakage</li> <li>• Employee training programs often inadequate or ineffective</li> </ul>	<ul style="list-style-type: none"> <li>• The cost of a breach can range from \$90 to \$305 per record</li> <li>• Costs may include legal counsel, mail notification, call center support, lost productivity fines to civil courts and other payments</li> <li>• Breach may also result in additional audit requirements, further exacerbating resources</li> </ul>	<ul style="list-style-type: none"> <li>• The impact from a cyber threat can have life endangering consequences or a public health impact, in addition to the obvious loss of data</li> <li>• Can affect the trust from the public for the government or agency, having long-lasting political implications</li> </ul>



**June 2010: Nantucket  
man arrested for  
operating international  
on-line ‘phishing’  
scheme to steal income  
tax refunds**

Source: US DOJ, Office of Public Affairs, June 24, 2010

Calls to action

# CSIS cybersecurity commission

## Summary of findings and recommendations (Dec 2008)

- Cybersecurity — now a major national security problem for the U.S.
- Decisions and actions must respect privacy and civil liberties
- Only a comprehensive national security strategy that embraces both domestic and international aspects of cybersecurity will make us more secure
  - Create a Comprehensive National Security Strategy for cyberspace
  - Organize for cybersecurity
  - Partner with private sector
  - Regulate for cybersecurity
  - Secure Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems
  - Use acquisition rules to improve security
  - Manage identities
  - Modernize authorities
  - Revised Federal Information Security Management Act (FISMA)
  - End division between civilian and national security systems
  - Conduct training for cyber education and workforce development
  - Conduct research & development for cybersecurity



# A new day — U.S. cyberspace policy



*“The United States must signal to the world that it is serious about addressing this challenge (cybersecurity) with strong leadership and vision...leadership and accountability for cybersecurity should be strengthened.”*

*44th President, May 29, 2009, on introducing his report, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure”*

- United States is at a crossroads — “cyberspace” underpins almost every facet of society
- Status quo no longer acceptable — United States must lead with strong leadership and vision
- Federal government to initiate a national public awareness and education campaign
- United States should develop a globally competitive workforce
- Federal government should reinforce cybersecurity partnership with private sector
- United States needs a cybersecurity strategy addressing the international environment
- United States needs comprehensive framework to coordinate federal, state, local, tribal, private sector, and international allies’ response to significant cyberspace events
- Federal, state, and local partners should identify procurement strategies to incentivize the market to make more secure products and services

# President's cyberspace policy review (May 2009)

## Near-term action plan

- Appoint NSC/NEC dual-role cybersecurity policy official and establish NSC directorate:
  - On December 22, 2009, The President named Howard Schmidt as Cybersecurity Coordinator — he will report to NSC at the White House and will coordinate the U.S. government's cybersecurity policy for both military and civilian agencies
- Prepare cybersecurity national strategy
- Designate cybersecurity as a Presidential key management priority with metrics
- Designate a privacy and civil liberties official to the NSC cybersecurity directorate
- Formulate policy — clarify roles, responsibilities, and agency authorities
- Initiate national public awareness and education campaign
- Develop an international cybersecurity policy framework and strengthen international partnerships
- Prepare cybersecurity incident response plan; enhance public-private partnerships
- Develop framework for research and development (R&D) strategies focusing on game-changing technologies
- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties, leveraging privacy-enhancing technologies

# President's cyberspace policy review (May 2009)

## Mid-term action plan

1. Improve process for resolving interagency disagreements
2. Use performance-based budgeting, using OMB program assessment framework
3. Expand key information age education programs and R&D
4. Expand and train the workforce
5. Determine best mechanisms to obtain strategic warning, maintain situational awareness, and inform incident response capabilities
6. Develop a set of threat scenarios and metrics for risk management, recovery planning, and R&D prioritization
7. Develop a process between government and private sector for preventing, detecting, and responding to cyber incidents

### White House cyberspace policy review

TABLE 3: MID-TERM ACTION PLAN

1. Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
2. Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
3. Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
4. Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
5. Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
6. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
7. Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
8. Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
9. Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
10. Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
11. Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
12. Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
13. Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
14. Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.

# President's cyberspace policy review (May 2009)

## Mid-term action plan (cont.)

8. Develop mechanisms for information sharing that address privacy and proprietary information and make information sharing mutually beneficial
9. Develop solutions for emergency communications
10. Expand information sharing with key allies about network incidents and vulnerabilities
11. Encourage collaboration between academic and industrial laboratories
12. Define goals for national and international standards bodies
13. Implement an "opt-in" array of interoperable identity management systems to build trust for online transactions to enhance privacy
14. Refine government procurement strategies and improve market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services

### White House Cyberspace Policy Review

TABLE 3: MID-TERM ACTION PLAN

1. Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
2. Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
3. Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
4. Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
5. Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
6. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
7. Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
8. Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
9. Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
10. Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
11. Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
12. Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
13. Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
14. Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.

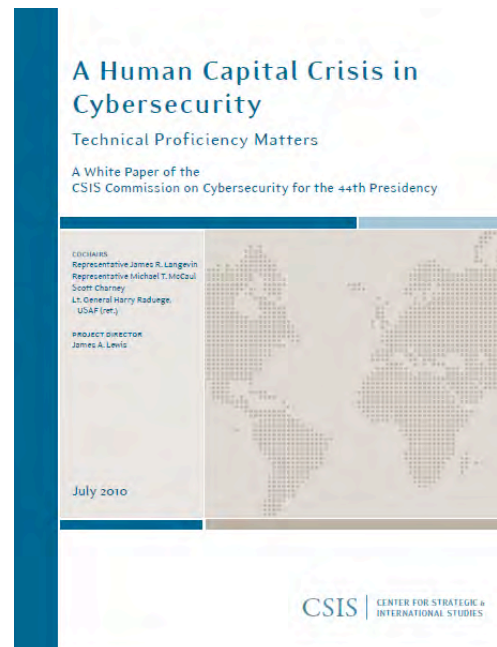
# CSIS cybersecurity commission (phase 2)

Began 24 Jun 09

*“ ... we will continue the Commission’s work to identify sound policies that address the critical issues for Cyberspace. We will build a national community of experts to engage in this vital task. Our goal is to fulfill the Commission’s vision for a secure Cyberspace while adhering to the bipartisan and independent principles that guided our report.”*

## Work plan and topics for phase 2 more detailed efforts:

- Authentication of identity
- Dynamic defense
- International engagement
- Privacy and civil liberties
- Workforce



## CSIS cybersecurity conclusion

The effort to improve cybersecurity offers the opportunity to rethink how government and industry operate and to build collaboration across organizational boundaries

The goal should not be the best defense, but government and industry that can:

- Securely take full advantage of cyberspace
- Enable and assure essential services in cyberspace
- Create opportunities for collaboration, growth, and national advantage



**2008:** 49% of global IT leaders believe that we are “falling behind” or “still catching up” to known security threats

**2009:** 60% of global IT leaders now believe...

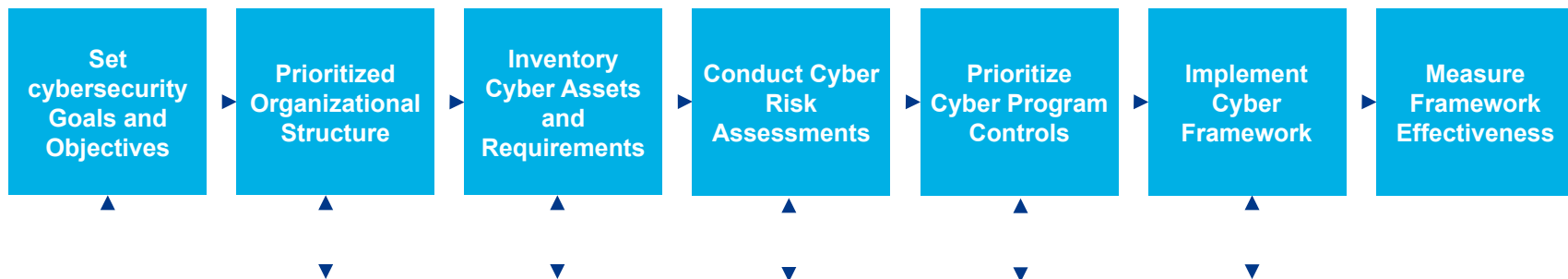


Source: Deloitte's 2009 Global Security Survey of the Technology, Media and Telecommunications

## Developing a "cyber mindset"

A cyber risk management approach is an example of a tool that can help an organization successfully achieve a cyber awareness culture.

Sample cyber risk management roadmap:



Road map allows continuous remediation, monitoring and improvement throughout

# Questions ?

# Deloitte.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2010 Deloitte Development LLC. All rights reserved.  
Member of Deloitte Touche Tohmatsu