



Succeeding in a cyber world

Cybersecurity Risks and Options for Improvement

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

August 15, 2011



Cyber — the phenomenon that changed the world

Cyber FININT Cyber Activism
Cyber-ethics Cyber War
Cyber attack Bullying Cyber Commerce
Cyber Law Cyber Communication
Security Law Cyber
Cyber Cyber
Espionage Cyber crime
Cyber-Alert

State of cybersecurity threats and ongoing challenges

What global leaders are thinking about cybersecurity...

54% doubt their organization is capable of defending itself against a sophisticated cyber attack

61% anticipate the impact of losing global connectivity for an extended period of time to be catastrophic with irreversible consequences

66% think home users need to take more responsibility for cybersecurity

66% view their government's maturity as low regarding international cooperation

66% a "treaty on cyber warfare" is needed or is overdue

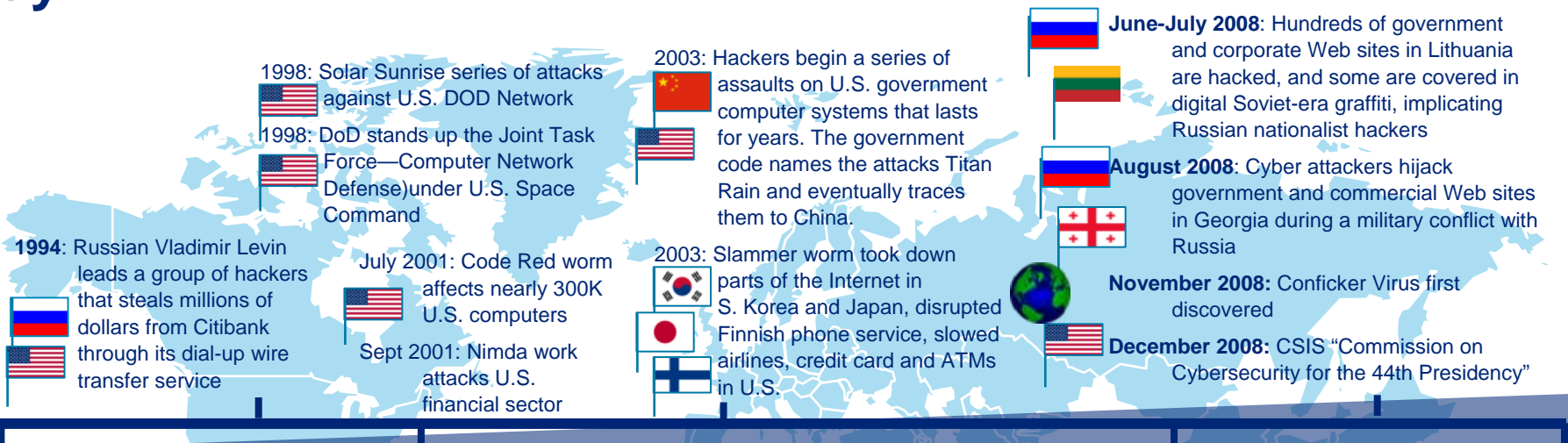
69% doubt their country could defend against a sophisticated cyber attack

70% believe that international policies and regulations are far behind technology advances

"Protecting the Digital Economy", East West Institute Report from the First Worldwide Cybersecurity Summit , May 2010

"Mobilizing for International Action", EastWest Institute Report from the Second Worldwide Cybersecurity Summit, June 2011

Cyber threats are borderless...



1979



1979: The first hacker forum emerges from a crude electronic messaging board

March 1999: Hackers in Serbia attack NATO systems in retaliation for NATO's military intervention in Kosovo

May 1999: NATO accidentally bombs Chinese embassy in Belgrade, spawning a wave of cyberattacks from China against U.S. government Web sites

1999: Moonlight Maze series of attacks against UD DOD computers

September 2003: DHS U.S. CERT established

April-May 2007: Hackers believed to be linked to the Russian government bring down the Web sites of Estonia's parliament, banks, ministries, newspapers and broadcasters

January 2009: Attacks shut down at least two of Kyrgyzstan's four Internet service providers

April 2009: An attack on neighboring Kazakhstan shuts down a popular news Web site

May 2009: White House "Cyberspace Policy Review"

December 2009: White House Cybersecurity coordinator appointed

May 2010: USCYBERCOM Stand up

May 2010: First Worldwide Cybersecurity Summit, Dallas, TX

June 2010: Stuxnet hits Iran

December 2010: DDoS WikiLeaks

December 2010: Lisbon Summit- NATO members agree on cyber cooperation

January 2011: CSIS "Commission on Cybersecurity for the 44th President" Progress Report

2011: Anonymous and LulzSec cyberattack campaigns against government and industry

2010

...U.S. response has been evolving

“Advanced cyber criminals have capabilities that approach those of national intelligence agencies...A flourishing black market supports cyber crime. In it, you can buy the latest malware, learn of recently discovered vulnerabilities, or rent “botnets” (thousands of computers remotely controlled for criminal purposes without the computer owners’ knowledge). Credit card numbers, personal information, and bank account data can be bought in bulk. Some sellers offer guarantees.”

Cybersecurity Two Years Later, CSIS Commission on Cybersecurity for the 44th Presidency, January 2011



White House Cybersecurity Legislative Proposal (May 2011)

Our Nation is at risk

- Protecting the American People
 - Data breach reporting; e.g. identity theft & personal information
 - Penalties for computer criminals
- Protecting the Nation's Critical Infrastructure
 - Voluntary Federal assistance to industry, states, & local government (when asked)
 - Voluntary information sharing with industry, states, & local government (with impunity)
 - Critical infrastructure cybersecurity plans with commercial auditor assessments
- Protecting the Federal Government Computers and Networks
 - Management; e.g. updating Federal Information Security Management Act (FISMA)
 - Personnel (flexible hiring & government /industry exchanges)
 - Intrusion prevention systems
 - Data centers (flexible “cloud” positioning)
- New framework to protect individuals' privacy & civil liberties
 - DHS & all agencies must follow privacy & civil liberties procedures
 - Monitoring, collection, use, retention, & information sharing must also follow procedures
 - Removal of personal information before information sharing
 - Layered oversight programs & congressional reporting
 - Immunity for private-sector business, state, or local government



Departments of Defense, Commerce, and State

2011 Policy Announcements

DoD

- **May 2011** – Declared cyberattacks an act of war under certain conditions
- **June 2011** – “Department of Defense Strategy for Operating in Cyberspace”
 - Leverage cyber workforce & rapid technological innovation to achieve DoD objectives
 - Cyberspace as an operational domain
 - Expand capabilities that protect against attacks
 - Increase cooperation with private sector & other agencies
 - Improve international cooperation for collective self-defense & deterrence

DoC

- **April 2011** – “National Strategy for Trusted Identities in Cyberspace (NSTIC)” – to create an “identity ecosystem” to authoritatively identify people, organizations, & infrastructure online
- **June 2011** – related report emphasizing economic importance of cybersecurity to protect global online transactions & maintain consumer trust in the internet

DoS

- **May 2011** – “International Strategy for Cyberspace” – The US will work with the private sector, allied nations, foundations, & civil society groups to:
 - Promote international economic standards for cyberspace
 - Enhance security, reliability, & resiliency
 - Extend collaboration & the Rule of Law
 - Cooperate militarily on cybersecurity
 - Promote effective & inclusive internet governance structures
 - Promote international freedom & privacy on the web

Center for Strategic and International Studies Commission on Cybersecurity: Cybersecurity Two Years Later Report

10 Outstanding Areas for Progress that Remain

- A **coherent organization** of Federal efforts for cybersecurity & recognition of cybersecurity as a **national priority**
- Clear authority** to mandate more effective cybersecurity in **critical infrastructure** & develop new ways to work with the **private sector**
- A **foreign policy** that uses a variety of tools of U.S. power to create norms, new approaches to governance, & consequences for malicious action actions in cyberspace. New policy should lay out vision & goals for the future of the global internet.
- An **expanded ability** to use intelligence & military capabilities for defense **against advanced foreign threats**
- Strengthened oversight for **privacy & civil liberties**, with clear rules & procedures adapted to digital technologies
- Improve **authentication of identity** for **critical infrastructure**
- Build an expanded **workforce** with acceptable cybersecurity skills
- Change **federal acquisition policy** to drive the market towards more security products & services
- A revised **policy & legal framework** to guide government actions
- Research & development (R&D)** focused on the hard problems of cybersecurity, & a process to identify these problems & investment opportunities in a coordinated manner

“The next Pearl Harbor we confront could very well be a **cyber attack** that **cripples our power systems, our grid, our security systems, our financial systems, our governmental systems...** This is a **real possibility** in today’s world...As a result, I think we have to aggressively be able to counter that. It is going to take both **defensive** measures as well as **aggressive** measures to deal with it.”



- Leon Panetta, Secretary of Defense

Cyber @ Heath & Human Services

Increasing technology and risk

The Latest Legislation & What it Means

•Health Information Technology for Economic & Clinical Health Act (HITECH Act) - modifies Health Insurance Portability & Accountability Act (HIPAA)

- Provides incentives for adopting electronic health record (EHR) systems & widens Privacy & Security Rules
- Mandates penalties for non-compliance with Privacy & Security Rules
 - Business Associates now held accountable
- Data breach notification requirements –covered entities must be notified of Protected Health Information (PHI) breaches (loss of greater than 500 PHI files must alert Federal HHS)
- Federal HHS can impose an ad hoc HIPAA assessment for any covered entity

•Health Insurance Exchange (HIX)

- Initiative under the Patient Protection & Affordable Care Act; establishes health provider marketplaces where consumers can pick from a variety of plans; run by state governments
- Federal HHS released guide for helping states set up HIX (11 July 2011)
 - Key initiative for health care reform

•Health Information Exchange (HIE)

- Office of National Coordinator for Health Information Technology offers grants for establishing independent and statewide HIEs.
 - HIE is a secure, electronically available health information network across a state, region, or hospital

NASCIO-Deloitte Cybersecurity Study

2010 Deloitte-NASCIO Cybersecurity Survey

- Leveraged Deloitte’s global security surveys and tailored for State government to assess key aspects of information security in States
- A State CISO survey review team, consisting of the NASCIO members & the Security and Privacy committee, reviewed & refined survey questions
- Most surveys completed using a secure online tool
- Data collection, analysis and validation was conducted by DeloitteDEX (Deloitte’s proprietary survey and benchmarking service)
- Results were analyzed according to industry leading practices & reviewed by NASCIO and senior members of Deloitte’s Technology Risk Services
- Further study compares State responses against Deloitte’s financial services bellwether survey & other external sources and benchmarks
 - Comparisons demonstrate divide between the private sector & States

49 States participated!

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Key Findings: 2010 Deloitte-NASCIO Cybersecurity Study

Governance: State leadership plays an important role in establishing:

- Top visibility for cybersecurity
- Chief Information Security Officers (CISO) have authority to be effective

Strategy: Sound security is not enough

- Must have an executable roadmap aligned to the business

Budget: Security budgets and resources available to State CISOs lag behind those of their private-sector counterparts

- Gap may be widening as the private sector is increasing security investments

Internal and External threats: States are struggling to keep up with security threats from organized & sophisticated cybercrime rings

Third party providers: States use the contractors services, managed service providers, & other third parties to deliver sensitive and critical constituent services

- Managing third-party security providers may not be keeping pace with escalating threats



This presentation contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this presentation, rendering business, financial, investment, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.