Caught in the Federal Procurement Fish Bowl
26th Annual Ounce of Prevention Seminar

Cyber Tsunami 2.0: Digital Pearl Harbors, Cyber Riptides, & Swirling Cybersecurity Standards

David Z. Bodenheimer
Crowell & Moring LLP

May 26-27
Newseum
Washington, DC
Urgency for Cyber Defense

The Cyber Crisis is **Now!!** – Everyone Agrees

**Congress**: “time to combat cyber terror was yesterday”  
(Senators Rockefeller & Snowe, May 29, 2009)

**Whitehouse**: “This status quo is no longer acceptable”  
(President Obama, May 29, 2009)

**Industry**: “Quite frankly, the bad guys are winning”  
(Cyber Security Industry Alliance testimony, Mar. 12, 2008)

**Cyber Report**: “one of the most urgent national security problems”  
(CSIS Commission on Cybersecurity, Dec. 2008)
Signs of the Cyber Apocalypse
74% Expect Foreign Attack

Cyber 9/11 on Banks

(8) According to the National Journal, Mike McConnell, the former Director of National Intelligence, told President Bush in May 2007 that if the 9/11 attackers had chosen computers instead of airplanes as their weapons and had waged a massive assault on a United States bank, the economic consequences would have been "an order of magnitude greater" than those caused by the physical attack on the World Trade Center. Mike McConnell has subsequently referred to cybersecurity as the "soft underbelly of this country".

S.773, § 2 “Findings”
38 Terabytes of Lost Data

2x Library of Congress

“As an example of the threat, one American company had 38 terabytes of sensitive data and intellectual property exfiltrated from its computers – equivalent to nearly double the amount of text contained in the Library of Congress.” [Sen. Whitehouse]
354 Million Breaches

91 Million Records Breached in One Year

Records with sensitive personal information involved in security breaches in U.S. since Jan. 2005:

354,320,320 records
May 7, 2010

262,424,592 records
June 4, 2009

[www.privacyrights.org]

PERSONAL DATA PRIVACY AND SECURITY ACT OF 2009

DECEMBER 17, 2009.—Ordered to be printed

Mr. LEAHY, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany S. 1490]

“According to the Privacy Rights Clearinghouse, more than 340 million records containing sensitive personal information have been involved in data security breaches since 2005.”
Trillion-Dollar Losses: “Business is currently on the front lines of a raging cyber war that is costing trillions of dollars and endangering our national security.” [ANSI & Internet Security Alliance, 2010]

“$1 trillion globally in lost intellectual property and expenditures for repairing the damage” (House Homeland Security Committee Hearing, Mar. 31, 2009)
No Safe Harbors for Anyone

Hackers Hit the Whitehouse

“Source In Iran Sees Plans for President’s Chopper” (USA Today, Mar. 2, 2009)

“The U.S. Navy is investigating how an unauthorized user in Iran gained online access to blueprints and other information about a helicopter in President Obama’s fleet.”

Hacking Obama’s Website

“It’s no secret that my presidential campaign harnessed the Internet and technology to transform politics. What isn’t widely known is that during the general election hackers managed to penetrate our computer systems.”

(President Obama, May 29, 2009)
No Safe Harbors for Anyone

“U.S. Supreme Court: Justice Breyer and Several Lawyers Were Victims of Data Breach” (ABA Law News, July 9, 2008)

“Navy CIO's PII Exposed for Sixth Time”

[Robert Carey, Navy CIO]

“The personal identifiable information of the Navy chief information officer has been compromised, again. And, it isn't just the second or third or fourth or even fifth time Robert Carey's PII has been exposed, but the sixth instance.”

[Gov Info Security, Jan. 4, 2010]
Cybersecurity: Pending Legislation, Regulation & Policy in 2010
Pending Cyber Legislation

Key Cyber Bills

• S. 773 Cyber Security Act
• S. 778 Cyber Czar
• S. 921 FISMA Update
• H.R. 4900 FISMA Update
• S. 3193 State Dept. Czar
• S. 3155 Global Cyber Threat Assessment

“There are already several dozen cybersecurity-related bills before Congress.” [Sen. Whitehouse, National Law Journal, May 10, 2010]
Pending Cyber Legislation

**Cybersecurity Act of 2010**

- RFP mandate for cybersecurity factors for IT procurements
- IT critical infrastructure standards, audits, & corrective action
- Private sector access to classified information
- NIST responsibility for cyber standards development
- National licensing & certification for cyber professionals
- NSF support for R&D & testbeds
- Public-Private Cyber Clearinghouse for threats & vulnerabilities (including access)
- Collaborative public-private emergency preparedness & response

111TH CONGRESS 1ST SESSION

S. 773

[Report No. 111-]

To ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cyber security defenses against disruption, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 1, 2009

Mr. ROCKEFELLER (for himself, Ms. Snowe, and Mr. Nelson of Florida) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

APRIL ——, 2010

Reported by Mr. ROCKEFELLER with an amendment in the nature of a substitute

[Strike all after the enacting clause and insert the part printed in italics]

A BILL

To ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cyber security defenses against disruption, and for other purposes.

© Crowell & Moring LLP 2010
Pending Cyber Legislation

Press Release for S. 773

National Cable & Telecomm Ass’n. “Passage of the Rockefeller-Snowe Cybersecurity Act is a necessary and important step . . .”

US Telecom. “The Rockefeller-Snowe bill takes positive and strategic steps . . .”

Verizon. “The legislation drafted by Senators Rockefeller and Snowe puts the nation on a much stronger footing to confront these threats.”

Symantec. “The Committee’s rigorous open stakeholder process has resulted in a much improved measure . . .”

REVIEWS ARE IN
ON ROCKEFELLER-SNOWE CYBERSECURITY ACT

Pitching Cybersecurity Bill as If It Were a Movie

March 26, 2010 - Eric Chabrow

“Are Rockefeller and Snowe the latest Astaire and Rogers, Tracy and Hepburn and Newman and Redford, Washington’s version of Hollywood blockbuster pairings? That’s an imaginative takeaway of a reading of a press release distributed Thursday by the Senate Commerce, Science and Transportation Committee that reads like the words of a Hollywood press agent with the headline.”
Proposed Regulations

DFARS Issues

• New Data Category. Adds new form of sensitive, but unclassified, information
• Encryption. Includes requirement for encryption (but no standard)
• Consistency. Establishes security standards (but does not incorporate NIST standards)
• Subcontract Flowdowns. Requires flowdowns (but does not provide clear standards)
• Intrusion Reporting. Specifies reporting of security breach (but does not centralize reporting)

DFARS ProposedRegs


[Text of DFARS Proposed Regulations]

© Crowell & Moring LLP 2010
Cybersecurity: Gambles, Puzzlers & Disputes for Contractors
Past Performance

Security Breach in Protests

“However, the USAJOBS screenshot, memoranda from OPM and OMB discussing the Government’s policy on safeguarding social security numbers, and the three sets of internet articles addressing Monster’s past security breaches ensure the completeness of the administrative record and shall be admitted.”


CIO TODAY

Monster Hackers Also Hit USAJobs.gov (Aug. 31, 2007)

“It now appears that Monster.com knew about a breach of its systems almost a month before Symantec told Monster of a massive phishing operation targeting Monster.com users. That long of a lag is "inexcusable," said W. David Stephenson, a homeland security and corporate crisis management consultant, "after the legacy of past problems."
“The proposal will be evaluated for an effective plan and timeline to meet the DoD DIACAP documentation requirements within allowed timeframes.”

S. 773 Rules for Future RFPs

4 SEC. 200. FEDERAL SECURE PRODUCTS AND SERVICES ACQUISITIONS.
6 (a) ACQUISITION REQUIREMENTS.—The Administrator of the General Services Administration, in cooperation with the Office of Management and Budget and other appropriate Federal agencies, shall require that requests for information and requests for proposals for Federal Information systems, products and services include cybersecurity risk measurement techniques, risk management measures, and best practices recognized under section 204 and the cybersecurity professional certifications recognized under section 101 of this Act.
16 (b) ACQUISITION COMPLIANCE.—After the publication of the requirements established by the Administrator under subsection (a), a Federal agency may not issue a request for proposals for Federal Information systems products and services that does not comply with the requirements.
Contractor Liability on Defense

What Happens When You Sell IT Security that Fails?

- **Gov. Contractor Defense**
  - Commercial specifications

- **SAFETY Act Coverage**
  - No terrorist attack

- **85-804 Indemnification**
  - Limited agency authority

- **Pending Legislation**
  - Political limitations

---

Boyle v. UTC, 487 US 500 (1988)
## Contractor Liability on Offense

### Going on the Offensive: Contractors in Cyber War

- **International Law**
  - Authority to attack?

- **U.S. Law**
  - Electronic surveillance & wiretapping laws
  - Covert operations (Title 10 vs. Title 50)
  - Posse Comitatus (DoD & domestic operations)
  - 5th Amendment takings

### $50 Billion Lawsuit

*Privacy Law Watch*

“One lawsuit alone, filed May 12 by a purported national class of Verizon customers, seeks $50 billion in damages ([95 PRA, 5/17/06](#)).”

[“Court Will Decide State Secrets Issues First in NSA Phone Surveillance Class Action Suit,” *Privacy Law Watch*, June 9, 2006]
<table>
<thead>
<tr>
<th>Types of Disputes</th>
<th>Cyber Disputes Act?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Denied Network Access</strong></td>
<td>• <strong>Real-time resolution</strong></td>
</tr>
<tr>
<td>– Threats to “pull the plug”</td>
<td>– Balance security risks &amp; contractor rights</td>
</tr>
<tr>
<td>– Cyber forfeiture &amp; debarment</td>
<td>• <strong>Specialized cyber expertise</strong></td>
</tr>
<tr>
<td><strong>Arbitrary Security Demands</strong></td>
<td>– Greater technology focus</td>
</tr>
<tr>
<td>– <em>Ad hoc</em> &amp; expensive add-ons</td>
<td>– Like GSBCA &amp; Brooks Act?</td>
</tr>
<tr>
<td>– “My way or the highway”</td>
<td>• <strong>High-stakes risks</strong></td>
</tr>
<tr>
<td><strong>Increased Vulnerabilities</strong></td>
<td>– Security vs. forfeiture</td>
</tr>
<tr>
<td>– Bad monitoring = open door</td>
<td>• <strong>Non-contract disputes</strong></td>
</tr>
<tr>
<td><strong>Disrupted IT Systems</strong></td>
<td>– 85% infrastructure in private hands</td>
</tr>
<tr>
<td>– Red-team disruptions</td>
<td>– Beyond Contract Disputes Act</td>
</tr>
</tbody>
</table>

© Crowell & Moring LLP 2010
# Public-Private Partnerships

## Partnerships Crucial

- **President Obama (2009).** “Third we will strengthen the public/private partnerships that are crucial to this [cybersecurity] endeavor.”

- **Sen. Rockefeller (2009).** “We need a coordinated public-private response. Currently, this does not exist.”

- **DNI Director Blair (2010).** “Acting independently, neither the U.S. government nor the private sector can fully control or protect the country’s information infrastructure.”

## Partnership Factors

- 85% IT infrastructure in private sector
- DoD Defense Industrial Base Model (bilateral model)
- Critical Infrastructure Models (multilateral model)
- Pending Legislation
Investigations, Oversight & Suits

Oversight Everywhere

• Congressional Hearings
• GAO Reports
• IG Investigations
• Criminal Sanctions
• Civil Penalties
• State Attorney General Suits

Thompson, Langevin Demand Investigation into Department Cyber Attacks (Sept. 24, 2007)

Over the previous five months, the House Committee on Homeland Security has investigated the information technology security posture at the Department of Homeland Security. The results of our investigation suggest that the Department is the victim not only of cyber attacks initiated by foreign entities, but of incompetent and possibly illegal activity by the contractor charged with maintaining security on its networks. We ask you to immediately commence an inquiry into these matters, and, if necessary, refer this matter for criminal investigation.

“criminal investigation”

We request that you initiate an investigation into these incidents and the actions of the contractor. As you know, 18 U.S.C. 1001 makes it a crime to knowingly and willfully make a materially false, fictitious or fraudulent statement or representation to the United States government. If your investigation determines that violations of Federal law may have occurred, we expect that you will provide this information to the appropriate officials at the U.S. Department of Justice. We also request a review of the actions of government officials responsible for overseeing this contract to determine whether any breaches of duty occurred. Finally, we are disappointed by the Department’s misleading responses to the Committee’s requests for information, and request that you determine whether the intent of these misstatements was to obstruct the Committee’s investigation.

“fraudulent statement”

© Crowell & Moring LLP 2010
New Cyber Czar


“Seven months after President Obama vowed to "personally select" an adviser to orchestrate the government's strategy for protecting computer systems, the White House will name a former Bush administration official to the job Tuesday.

Howard A. Schmidt, who was a cyber-adviser in President George W. Bush's White House, will be Obama's new cybersecurity coordinator, an administration official said Monday night.”

Mr. Schmidt’s Resume

- President, Information Security Forum (non-profit consortium)
- Special Advisor, National Strategy to Secure Cyberspace (2001-03)
- Chief Security Officer, Microsoft
- Chief Information Security Officer, eBay
- Active-duty & Civilian, Air Force
- Head, FBI National Drug Intelligence Center
“My administration will pursue a new comprehensive approach to securing America’s digital infrastructure. This new approach starts at the top with this commitment from me: From now on, our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority.”

(President Obama, May 29, 2009)
Congressional Cyber Scrutiny

Congressional Pressure (2008-2009 Actions)

- Congressional Scrutiny
  - Over 30 Hearings & Actions
  - 9 Different Committees

- GAO Reviews
  - Congress’ Investigative Arm
  - 22 Reports on Cyber Issues

- Legislative Actions
  - Senate Bill (S. 773)
  - House Bill (H.R. 2195)

FOR IMMEDIATE RELEASE

Statement of Chairman Bennie G. Thompson

“Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure”

April 10, 2007 (Washington) – Today, Committee on Homeland Security Chairman Bennie G. Thompson (D-MS) delivered the following prepared remarks for the Emerging Threats, Cyberspace, and Science and Technology Subcommittee hearing entitled “Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure”.

“I’ve been tracking this issue for some time now. In October 2006, when the world first learned of the hacking incident at the Department of Commerce, I sent a letter to the Assistant Secretary for Cybersecurity, Greg Garcia, asking several specific questions about the role of the Department in responding to this incident.

Unfortunately, I never received a response back from the Department. I understand that I’m not the only one being left in the dark when it comes to the Department’s efforts in cyberspace. If understand Chairman Langevin correctly, many federal agencies are waiting for the Department to provide them with timely intelligence and recommendations about hacking incidents at the federal level.

Many in the private sector are also telling me that the Department is failing to provide the guidance and partnership necessary to successfully secure cyberspace. It is clear that our government, working together with the private sector and academia, must do more to ensure that cybersecurity is a priority in our nation’s homeland security strategy.

In 1996, the United States government undertook the first national effort to secure our networks. Unfortunately, I don’t believe that we are any further along today in our efforts to secure cyberspace.

Programs and initiatives that were developed over the past ten years have been dismantled and, in certain instances, are just now being re-created by the government. We can see that the Administration views its priorities in cyberspace differently from the last Administration.”
Cyber Goes Global: International Risks & Issues
International Attacks

“Did China Copy U.S. Commerce Secretary’s Laptop Computer?” “Surreptitious copying is believed to have occurred when a laptop was left unattended during [Commerce Secretary Carlos] Gutierrez’s trip to Beijing for trade talks in December.” (ABA Law Journal News, May 29, 2008)

Cross-Border Transfers

“B.C. civil servant accused of sending personal data to U.S. border guard”

Global Security Initiatives


“The new provisions will bring vital improvements in the protection of the privacy and personal data of all Europeans active in the online environment. The improvements relate to security breaches, spyware, cookies, spam, and enforcement of rules.” (Internet Business Law Services, Dec. 22, 2009).

“In Shift, U.S. Talks to Russia on Internet Security”

“The United States has begun talks with Russia and a United Nations arms control committee about strengthening Internet security and limiting military use of cyberspace.” (NYT, Dec. 13, 2009)
Global Cyber Initiatives

Global Arms Race

“Cyber security the new ‘arms race’” Van Loan

“I really look at [cybersecurity] almost as the new arms race. There isn’t a day that goes by without someone somewhere trying to breach the Government of Canada’s information systems.”

(Public Safety Minister Van Loan, CTV News, May 27, 2009)
Questions?

David Z. Bodenheimer
Crowell & Moring LLP
dbodenheimer@crowell.com
(202) 624-2713