The Cyber Forecast -- Hotter Than Global Warming:

A Review of 2007 and Preview of 2008 in Cybersecurity

by

David Z. Bodenheimer

The Cybersecurity Forecast

Money

Breach

Oversight

The DC Cyber Security
Breakfast Series

Cyberspace & Homeland Security
Vulnerability & Opportunity

January 24, 2008
The Cyber Forecast -- Hotter Than Global Warming:

In the cyber realm, momentum is building – and the primary drivers are hemorrhaging security breaches, sizzling oversight, and mushrooming money. In fact, the relationship is virtually mathematical:

\[
\text{Security Breaches} \rightarrow \text{Oversight} \rightarrow \text{Money}
\]

In the past five years, cybersecurity has shifted from an IT insider’s worry to a popular media and political obsession. One way to track this trajectory at a glance is through the headlines:

**2005: The Year of Personal Information Insecurity**

“Hackers Tap 40 Million Credit Cards,” *Los Angeles Times* (June 18, 2005)

“Burned by ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance,” *Information Week* (Feb. 24, 2005)


**2006: The Year of Federal Information Insecurity**


“Navy Probes Data Leak on 100,000 Sailors, Marines,” *Reuters* (July 7, 2006)

**2007: The Year of Oversight for Information Insecurity**


“Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses,” GAO (July 27, 2007)

“Challenges Remain in Securing the Nation’s Cyber Infrastructure,” DHS Inspector General (June 2007)
I. Security Breach Forecast: Blizzard Conditions Will Worsen

By any measure, security breach has become everyone’s problem. For 2007, a blizzard of new security breaches have set new records for compromised personal information.

A. Security Breach & Cybercrime by the Numbers

Since 2005, security breaches have skyrocketed, exposing personal information in both government and private hands. Even at a glance, the numbers are sobering.

- **Sensitive Personal Information Records Breached**
  - 127 million records compromised in 2007\(^1\)
  - 600% increase over 2006\(^2\)
  - 217 million records breached since 2005\(^3\)

- **Cybercrime Costs**
  - $105 billion worldwide in 2007\(^4\)
  - Outstripped illegal drug trafficking

- **US CERT Data**
  - 37,000 incidents (Oct. 2006 to Sept. 2007)\(^5\)
  - 24,000 incidents (Oct. 2005 to Sept. 2006)
  - 54% increase (over 1-year period)

---

1  “2007 Data Breach Stats,” Identity Theft Resources Center (ITRC)  

2  “2006 Disclosures of U.S. Data Incidents,” ITRC (over 19 million potentially affected in 2006)  

http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP


http://www.dhs.gov/xnews/releases/pr_1197409593155.shtm
B. Private Sector Breaches & Vulnerabilities

- TJX Security Breach
  - 46 to 94 million records exposed\(^6\)
  - $40.9 million likely settlement with credit card company\(^7\)
  - $12 million earnings hit (1\(^{st}\) Quarter 2007)\(^8\)

- Breaches & Vulnerabilities
  - 85% data breaches (midsize & large businesses)\(^9\)
    - 59% faced potential litigation
    - 32% experienced decline in share prices
  - 21% of attacks cost over $100,000 (11% over $500,000)\(^10\)


- 3,930 commercial HAZMAT drivers

“Whacking Hackers,” Newsweek (Oct. 15, 2007)
- 1,500 Pentagon computers hacked, disabled

- FBI investigation of Chinese hacker break-in

“Monster Theft Also Hit Government Site,” USA Today (Aug. 31, 2007)
- 146,000 users’ contact information stolen from USAjobs.gov

“Lax and Lazy at Los Alamos,” Newsweek (June 25, 2007)
- Leak of highly classified data from nuclear lab

---


\(^7\) Jewell, “TJX to Pay Up to $41M over Data Breach,” Worcester Telegram & Gazette (Dec. 1, 2007).

\(^8\) “Asking for Trouble: Most Companies Don’t Have Plans to Handle Data Breach,” CMP TechWeb (May 22, 2007).

\(^9\) Id., citing Ponemon Institute survey.

II. **Cyber Oversight: Hail and Lightning Are Striking Hard**

In the information security business, oversight comes from all directions – Congress, GAO, Inspectors General, OMB, the courts – and more.

A. **Congressional Oversight**

Congress – particularly the House Homeland Security Committee – has been particularly active in exercising oversight through hearings, reports, and investigations of information security shortfalls and gaps for both federal agencies and the private sector.


B. Government Accountability Office (GAO) Reports

In 2007 and 2008, GAO’s information security reviews cut across nearly every federal agency and identified pervasive weaknesses in protection of highly-sensitive – and in some cases, classified – data.


“Information Security: Sustained Management Commitment and Oversight are Vital to Resolving Long-Standing Weaknesses at the Department of Veterans Affairs, GAO (GAO-07-1019)


“Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats,” GAO (GAO-07-705) (June 22, 2007)


“Bureau of the Public Debt: Areas for Improvement in Information Security Controls,” GAO (GAO-07-899R) (June 14, 2007)
http://www.gao.gov/new.items/d07899r.pdf


“Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” GAO (GAO-07-737) (June 4, 2007)

C. Inspector General (IG) Reports

The Offices of Inspector General for numerous agencies issued a host of reports in 2007 and 2008 criticizing information security. Examples from DHS and DOE include:

http://ig.energy.gov/documents/IG-0785.pdf

“Information Technology Management Needs to Be Strengthened at the Transportation Security Administration,” DHS OIG (OIG-08-07) (Oct. 2007)

“Better Administration of Automated Targeting System Controls Can Further Protect Personally Identifiable Information,” DHS OIG (OIG-08-06) (Oct. 2007)

http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-77_Sep07.pdf

http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-77_Sep07.pdf

“Challenges Remain in Securing the Nation’s Cyber Infrastructure,” DHS OIG (OIG-07-48) (June 2007)  

http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_07-24_Jan07.pdf

**D. Office of Management & Budget (OMB) Oversight**

Under FISMA, OMB has a statutory responsibility to oversee information security for federal agencies. 44 U.S.C. §§ 3541-49. In the most recent report to Congress, OMB said federal agencies have made progress. But the grades are still not very good.

<table>
<thead>
<tr>
<th>Agency</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency for International Development</td>
<td>Good</td>
</tr>
<tr>
<td>Department of Agriculture</td>
<td>Poor</td>
</tr>
<tr>
<td>Department of Commerce</td>
<td>Poor</td>
</tr>
<tr>
<td>Department of Defense</td>
<td>Poor</td>
</tr>
<tr>
<td>Department of Education</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Department of Energy</td>
<td>Poor</td>
</tr>
<tr>
<td>Environmental Protection Agency</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>General Services Administration</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Department of Health and Human Services</td>
<td>Good</td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Department of Housing and Urban Development</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Department of Justice</td>
<td>Poor</td>
</tr>
<tr>
<td>Department of Labor</td>
<td>Good</td>
</tr>
<tr>
<td>National Aeronautics and Space Administration</td>
<td>Poor</td>
</tr>
<tr>
<td>National Science Foundation</td>
<td>Good</td>
</tr>
<tr>
<td>Nuclear Regulatory Commission</td>
<td>Failing</td>
</tr>
<tr>
<td>Office of Personnel Management</td>
<td>Excellent</td>
</tr>
<tr>
<td>Small Business Administration</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Smithsonian Institution</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Social Security Administration</td>
<td>Excellent</td>
</tr>
<tr>
<td>Department of State</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Department of Transportation</td>
<td>Good</td>
</tr>
<tr>
<td>Department of the Treasury</td>
<td>Poor</td>
</tr>
<tr>
<td>Department of Veterans Affairs</td>
<td>Poor</td>
</tr>
</tbody>
</table>

| Total “Excellent”: 2 | Total “Good”: 6 | Total “Satisfactory”: 8 | Total “Poor”: 8 | Total “Failing”: 1 |

E. Litigation Oversight

Litigation follows money – and security breaches. As a result, companies in the cybersecurity business will increasingly see litigation swirling around all things cyber.

1. Potential Criminal Investigation & Prosecution

For both federal agencies and contractors, the stakes are increasing as failed cybersecurity may lead to criminal investigations and potential prosecution.

http://www.hsc.house.gov/press/index.asp?ID=268&SubSection=0&Issue=0&DocumentType=0&PublishDate=0

2. Protest Litigation

As more federal money flows into cybersecurity, competing contractors will become increasingly willing to protest awards involving information security technology. For example, GAO recently sustained a protest involving a Department of Justice (DOJ) solicitation for services to support information security programs. See Superlative Technologies, Inc., B-310489 et al., Jan. 4, 2008 (http://www.gao.gov/decisions/bidpro/310489.pdf)

3. Security Breach Litigation

Class-action lawsuits have been a common response to a security breach. For example, the American Federation of Government Employees (AFGE) filed a class action in the U.S. District Court in the District of Columbia against TSA for loss or theft of 100,000 payroll records of current and former employees. In the suit, the labor union alleged violations of the

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

Where DHS and its contractor did not take certain information security precautions, hackers penetrated the system, compromising dozens of computers and exfiltrating information to services connecting to Chinese websites.
security and confidentiality requirements under the Privacy Act, as well as the Aviation and Transportation Security Act. As Senator Lieberman pointed out, “TSA has compromised the information of airport security officers, air marshals and other TSA law enforcement officers.”

III. **Money for Cybersecurity: After a Drought Comes the Monsoon**

For years, independent commissions, security experts and others have called for more money for cybersecurity. For years, cybersecurity funding has remained relatively flat. However, 2008 and 2009 will see a substantial funding ramp-up for a number of reasons.

A. **Critical Infrastructure Protection**

Much of the burden for security falls upon the private sector which “controls 85 percent of the critical infrastructure in the nation.” National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, p. 398. Several statutory and regulatory developments will increase the impetus for private sector effort to bolster information security.

1. **Chemical Cybersecurity**

The Fiscal Year 2007 Homeland Security Appropriations Act imposed additional security requirements upon chemical facilities. Pub. L. No. 109-295, § 550. In the implementing regulations, DHS expressly required chemical facilities to address cybersecurity in their Site Security Plans:

The Department recognizes that cyber security is an issue and has included cyber security as one of the performance standards that facilities must address in their Site Security Plan. Paragraph (c)(8) requires facilities to select, develop, and implement measures that “deter cyber sabotage.” In addition, the Department notes that it has implemented an assessment of cyber vulnerabilities for industrial control systems within the CSAT Security Vulnerability Assessment.

72 Fed. Reg. 17706 (2007); 6 C.F.R. § 27.230(c)(8) (2007). With the issuance of Appendix A in November 2007 (72 Fed. Reg. 65396), chemical facilities will be preparing vulnerability assessments and security plans that will include steps to address cybersecurity.

2. **Surface Transportation Cybersecurity**

In the 9/11 legislation, Congress required certain rail and bus carriers to perform “vulnerability assessments and security plans” addressing the security of “information systems,” including “programmable electronic devices, computers or other automated systems” which are used in such transportation. Pub. L. No. 110-53, §§ 1512(d)(1) (railroad carriers) and 1531(d)(1) (bus carriers). In addition, the 9/11 Act authorizes $25 million per year (FY 2008-11) for “public

---

transportation research and development” grants that may be used for such purposes as “research technologies that mitigate damages in the event of a cyber attack.” Pub. L. No. 110-53, § 1409(c)(2)(F).

3. Power Grid Cybersecurity


B. IT Security Spending

For Fiscal Year (FY) 2008, the budget request seeks $66.4 billion for information technology, with IT security accounting for 9.2% – $6.092 billion – of this amount. This request reflects a slight upward trend in IT security funding:

![Cyber Security Increases](http://www.whitehouse.gov/omb/egov/documents/FY08_IT_Budget_Rollout_MayUpdate.pdf)
C. Cyber Priorities for 2008

For 2008, cybersecurity takes a front seat, with the President, DHS, and the Intelligence community all placing heightened emphasis on greater protection.

1. Additional Cyber Funding for FY 2008

In November 2007, President Bush asked for additional FY 2008 funds to be allocated to cybersecurity.12

THE WHITE HOUSE
WASHINGTON

November 6, 2007

Dear Madam Speaker:

I ask the Congress to consider the enclosed amendments to my FY 2008 requests for the Departments of Homeland Security and Justice. These amendments, when combined with funding enacted earlier this year for the FBI (Public Law 110–28), would provide $436 million to take important steps to enhance ongoing efforts for protecting the homeland. The amendments will enhance the security of the Government’s civilian cyber networks and will further address emerging threats.

Overall, the discretionary budget authority proposed in my FY 2008 Budget would not be increased. The details of these amendments proposal are set forth in the enclosed letter from the Director of the Office of Management and Budget.

Sincerely,

[Signature]

According to OMB’s budget breakdown, this FY 2008 amended request includes the following specific cyber efforts:

- “$39 million to assist FBI’s investigations of incursions into the Government’s cyber networks, increase relevant intelligence analysis, and provide the necessary technical tools that support both investigations and analysis”;

12 President Bush’s letter to Speaker Pelosi (Nov. 6, 2007) and supporting OMB rationale (http://www.whitehouse.gov/omb/budget/amendments/amendment_11_6_07.pdf).
• “$115 million for cybersecurity initiatives to enhance Federal civilian detection capabilities, including accelerated deployment of monitoring capabilities and increased analytical operations at United States Computer Emergency Readiness Team (US-CERT) to support civilian agencies.”

2. Top Homeland Security Priority

In December 2007, DHS Secretary Chertoff identified cybersecurity as one of his top four priorities for 2008.13 As part of this effort, he specifically identified initiatives for expanding the Einstein Program (for detecting malicious patterns in computer network traffic) and “working with Congress, as we speak, on an enhanced cybersecurity strategy, which I believe will set the template for the next decade on how we deal with this emerging and increasing threat.”

3. Intelligence Priority

Since his “info-sec epiphany” at NSA, Admiral Mike McConnell (Director of National Intelligence) has been a strong proponent of both cyber warfare and defense.14 During a meeting with President Bush in May 2007, Admiral McConnell warned that “[i]f the 9/11 perpetrators had focused on a single U.S. bank through cyber-attack and it had been successful, it would have an order-of-magnitude greater impact on the U.S. economy.” During that meeting, President Bush “charged McConnell to come up with a security strategy, not only for government systems but also for American industry and private individuals.” Based upon public sources, DNI’s “Cyber-Security Policy” remains in draft.15 To implement the President’s direction and DNI’s cyber policy, substantial additional commitments of resources and funding are inevitable, as Admiral McConnell seeks to make his mark on information security in his remaining year at DNI.

_________


15 Id.