crowell moring

Managing the Cybersecurity Threat

State of the Art Trade Secrets Protection Strategies
Washington, DC
Nov. 15, 2011

David Z. Bodenheimer
Partner
Crowell & Moring LLP

Cyber Spies Stealing US Secrets

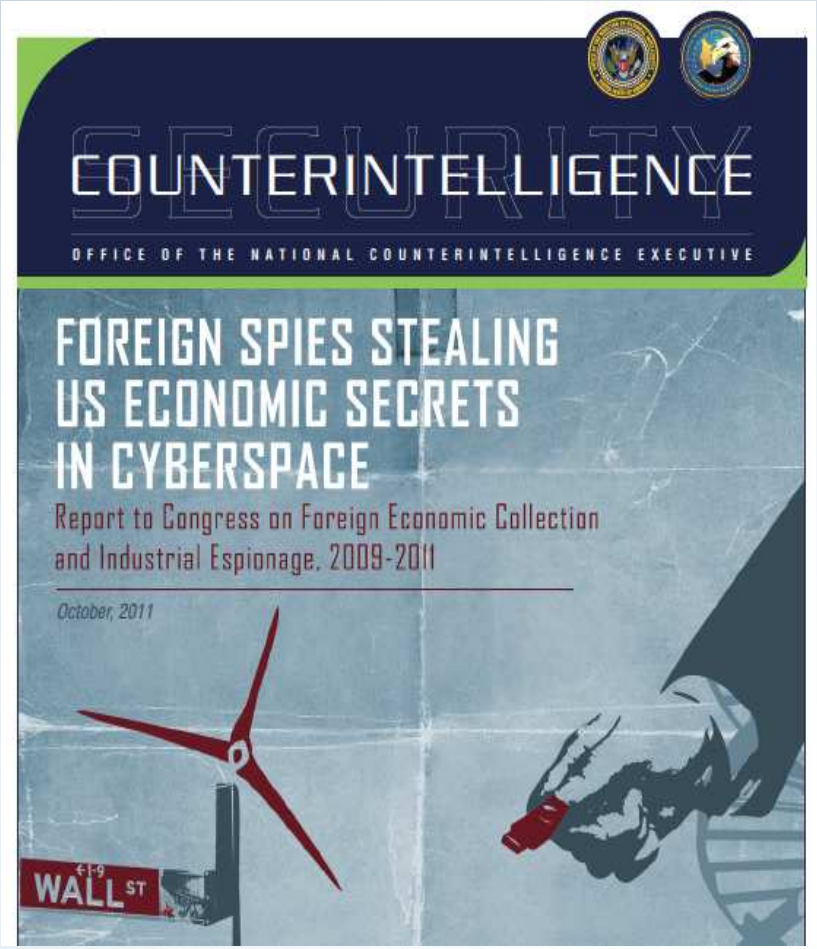
Cyber War on US Companies

» **Who's Stealing our Technology?**
- China, Russia and even our allies

» **What are the Primary Cyber Targets?**
- IT & Communications technology
- Natural resources data
- Military technologies
- Dual-use technologies (*e.g.*, clean energy & healthcare/pharma)

» **How are US Companies Hurt?**
- Wasted R&D investments
- Eroded profitability (1/8 of Valspar's profits)
- Lopsided negotiations

Intelligence Report



Cyber Risks – SEC Scrutiny

Security Problem

- Not disclosing material risks

Impact

➔ SEC scrutiny or actions

"Cyber risk management is a critical corporate responsibility. Federal securities law requires publicly traded companies to disclose 'material' risks and events, including cyber risks and network breaches. A review of past disclosures suggests that a significant number of companies are failing to meet these requirements." [Senate Commerce News Release, May 12, 2011]

U.S. Senate Committee on Commerce, Science, and Transportation

SEC Disclosure Duty

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2 Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents

Disclosure Duties

- **Risk of Cyber Incidents**
- **Prior Security Breaches**
- **Adequacy of Preventative Measures**

Cyber Risks – Shareholders

Security Problem

- Risking personal data

Impact

➔ Shareholder or private suits

$20 Million Suit. Countrywide's lax "internal procedures" & security breach [Courthouse News, Apr. 5, 2010]

Stock-Price Hit. "Sony fell **2.3 percent** to 2,262 yen" after security breach of 101 million records. [Bloomberg News (May 6, 2011)]

$6.75 Million/Incident. "average cost per incident of a data breach" in U.S. [Sen. Comm. Hearings, Sept. 2010]

Sony Breach – 101 Million

"In addition to **losing** an estimated revenue stream of **$10 million a week**, Sony will probably have to reimburse customers who pay for its premium service, rebuild its computer systems and **beef up security measures**, said Michael Pachter, an analyst with Wedbush Securities who said the incident could cost the company $50 million." [*L.A. Times,* Apr. 28, 2011]

Cyber Risks – Lost IP

Security Problem

- Insufficient data monitoring

Impact

➔ 38 terabytes of lost data

"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, May 10, 2010]

2 x

Bet-the-Company

$1 Trillion Losses. "Cyber criminals stole intellectual property from businesses worldwide worth up to **$1 trillion**." [President Obama, 2009]

$$

"Greatest Damage." "The greatest damage to the American economy from cyber attacks is due to massive thefts of business information." [Scott Borg (Dir., U.S. Cyber Consequences Unit)]

$$

$400 Million Theft. "A single employee of an American company was convicted of stealing intellectual property reportedly worth **$400 million**." [President Obama, 2009]

Cyber Risks – Suspension

Security Problem

- Misuse of DoD data (wrong purpose)

Impact

➔ Suspension

➔ Loss of $5B Contract

"But earlier this month the deputy general counsel of the U.S. Air Force suspended the L-3 unit responsible for the work from receiving new orders because of the investigation. Employees at L-3's special support programs division were accused of copying government emails and forwarding them without the author's knowledge."

Tuesday, June 22, 2010 As of 1:22 PM EDT

THE WALL STREET JOURNAL.

L-3 Trips as Lockheed Snatches $5 Billion Contract

"A disputed U.S. military contract worth up to $5 billion was finally awarded to Lockheed Martin Corp. (LMT) this week after the U.S. Air Force launched an investigation into possibly inappropriate email activities at rival L-3 Communications Corp. (LLL).

L-3, a New York-based provider of military and aerospace equipment, reduced its 2010 outlook as a result of the lost contract, which represented about 3% of its 2009 revenue, according to a government filing. Full-year profit is now expected to be in a range of $8.09 to $8.29 a share, compared to a prior view of $8.13 to $8.33 a share."

Pre-Breach Security Safeguards

Prevention/Safeguards

- Inventory IP/trade secrets
  - What & where
- Assess vulnerabilities
  - Breach risk assessment
- Benchmark current security vs. new standards
- Control Relationships
  - Vendors & supply chain
  - Customer solicitations
  - Teammates & NDAs

More Safeguards

- Limit access to IP/Secrets
  - Need to know
- Use security controls
  - Technical, physical, admin.
- Train, train, train
  - Privacy, security & breach ID
- Use detection technology
- Dispose of data properly

Post-Breach Safeguards

Incident Response Plan

- Security IR Team (SIRT)
- Templates (*e.g.*, notices)
- Critical contracts
- Notification deadlines
- Pre-vetted entities
- Contact lists: vendors, clients, authorities
- Escalation plan: who, what, when within company

Taking Action

- Secure the information/systems
- Conduct investigation
- Involve law enforcement
- Categorize data lost
- Document incident & response
- Be prepared with public statement
- Be consistent in statement, policy & practices
- Prepare for inquiries (policies, contracts & audits)
- Letters to individuals, authorities & credit reporting agencies
- Call Center FAQs/Call Script
- Vendor: Creditor monitoring

Questions?

David Z. Bodenheimer

Crowell & Moring LLP

dbodenheimer@crowell.com

(202) 624-2713