SIDLEY AUSTIN LLP

SIDLEY

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG HOUSTON LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

Cybersecurity: Corporate Responsibility and Governance

Edward R. McNicholas
Alan Charles Raul
Jeffrey S. Rothstein

January 2013

Corporate Data at Risk

- DHS announcement in May 2012 of ongoing, coordinated cyber attack on the control systems of U.S. gas pipelines
- NCIX report in 2011 detailing economic cyber sabotage against U.S., originating in China or Russia
- 2011 hack of top secure identity management firm RSA through phishing emails
- Hack in 2011 of NASDAQ "Directors Desk" portal with confidential board materials for public companies
- McAfee's claim in 2011 that Chinese hackers responsible for cyber attacks on 72 international firms and the UN over a 4 year period
- DoD revelation in 2010 of upload in 2008 of malicious code from flash drive onto networks containing classified information run by U.S. Central Command and government contractors
- Spike in industrial espionage reported by NCIX to cost as much as $400 billion each year

What's at Stake?

Valuable IP assets, proprietary information, business, transaction and negotiating records, financial data, electronic funds, business functionality and continuity

SCADA (supervisory control and data acquisition):

- industrial control systems (ICS): computer systems that monitor and control industrial, infrastructure, or facility-based processes

Account information; personal information; access to accounts

Supply chain management

Disruption of business; denial of service; cyber-extortion

Communication systems

Debilitating impact on critical infrastructure and essential services

Data Security: On the Corporate Radar?

- FTI Consulting/Corporate Board Member Survey:
  - Data security is **a top legal concern** in 2012 for both Directors and General Counsel
    - The percentage of Directors and GCs concerned re: data security has **doubled** since 2008
  - The median annualized cost of cyber-crime per company averaged $5.9 million
  - The survey noted participants' opinion that cyber risks are invisible, ever-changing, pervasive, and costly
  - But: only 42 percent of survey participants said their company had a data crisis management plan in place

Corporate Practices on Cybersecurity: Report Suggests Lack of Board Involvement

Boards of Energy/Utility Companies

- 71% rarely or never review privacy and security budgets
- 79% rarely or never review roles and responsibilities
- 64% rarely or never review top-level policies
- 57% rarely or never review security program assessments

Boards of Financial Sector Companies

- 42% rarely or never review annual privacy/security budgets
- 39% rarely or never review roles and responsibilities
- 56% do not actively address computer/information security
- 52% do not review cyber insurance

Governance of Enterprise Security: CyLab 2012 Report

Enhance Board/CEO Attention

- Review and refine information governance structure
  - Assign distinct board committee responsibility for cybersecurity, data protection and information privacy; establish expectations for management; require ongoing reporting regarding information risks and controls; review top-level policies
  - Assign C-level management responsibility, accountability and reporting obligations; provide adequate budget and operational resources; authorize involvement in industry/government information sharing
  - Consider appointing CISO (chief information security officer) and CPO (chief privacy officer)
  - Develop and approve appropriate cybersecurity protocols and safeguards; increase internal awareness
- Evaluate cyber-insurance coverage

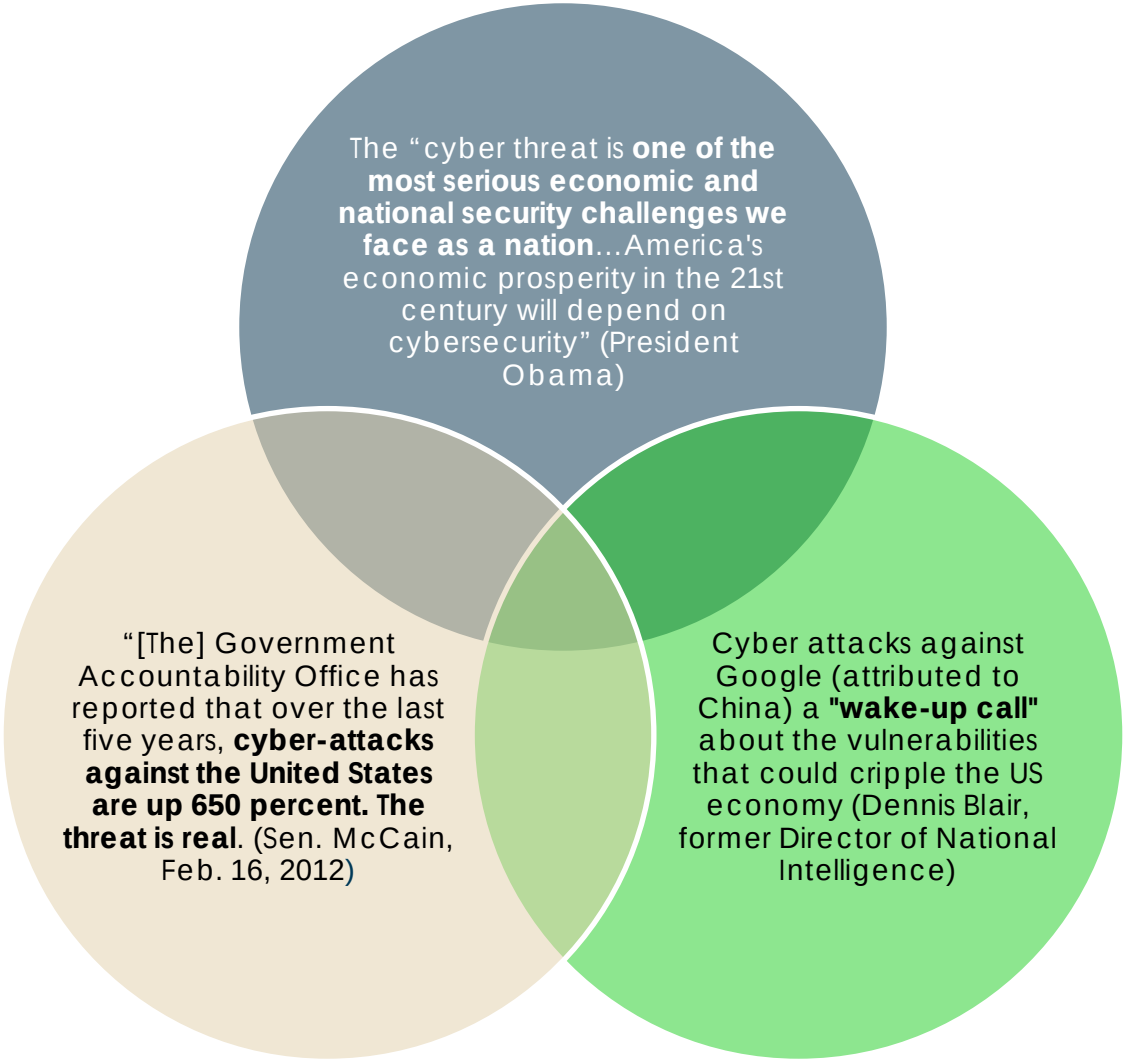
Enhance Board/CEO Attention – cont'd

- Develop cybersecurity and data protection risk assessment
  - Understand system and network vulnerabilities; plan for possible "persistent" threats
  - Understand exposure of essential or valuable information and communication assets
  - Understand exposure to third parties and service providers
  - Consider possible counter-measures to disrupt or divert attacks
- Monitor legislative, policy, industry, contractual, litigation, marketplace, consumer and employee developments and expectations
  - Address legal compliance and reporting responsibilities
  - Consider SEC issues
- Engage IT and audit experts; test systems

Responding to an Incident

- Effectuate IT containment and triage
- Assess nature of attack; IP assets; trade secrets; financial; customer data; denial of service; geopolitical; hacktivists
- Determine affected systems and targeted data; gauge possible exfiltration; address persistent threats
- Involve outside counsel and forensic IT consultants?
- Identify and notify stakeholders?
- Consult government; national security; law enforcement; homeland security?
- Assess liabilities, legal compliance, contract obligations, SEC reporting, insurance, etc.
- Evaluate existing control systems, responsibility and accountability; implement lessons learned

US Government Perspectives on Cybersecurity



SIDLEY AUSTIN LLP
SIDLEY

US Perspectives on Cybersecurity Cont'd

- "Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets."
- "Cyber tools have enhanced the economic espionage threat, and the Intelligence Community (IC) judges the use of such tools is already a larger threat than more traditional espionage methods."
- "Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries [especially China and Russia]."

Report from the Office of National Counterintelligence Executive (NCIX), October 2011

SIDLEY AUSTIN LLP
SIDLEY

Litigation Exposure

- **Customer whose bank funds were stolen by hackers alleged that bank holding did not do enough to prevent hack**
  - *Patco Construction Co. v. People's Ocean Bank* (D. Me.) (summary judgment granted to def., 2011)
  - *Anderson v. Hannaford Bros.:* Hack of credit card magnetic strip; merchants have implied contractual duty to safeguard customer financial data
- **Bank sued to avoid refunding customers funds taken from their account by Romanian hackers with valid credentials**
  - *PlainsCapital Bank v. Hillary Machinery, Inc.* (E.D. Tex.) (settled, 2010)
- **Data breach litigation following cyber attacks**
  - E.g., class actions filed against Sony after PlayStation hack
- **Failure to safeguard could expose boards to shareholder suits alleging negligence or breach of fiduciary duty**
  - Delaware *Caremark* decision: duty of care to safeguard digital assets

Congress on Cybersecurity

- Numerous bills proposed in last Congress; none passed
- Minimal consensus that critical infrastructure must be protected
  - utilities, electrical grid, telecommunications, financial services, defense contractors
  - facilitate information sharing
- National Defense Authorization Act for FY 2013 (signed Jan. 2, 2013) requires defense contractors with security clearances to notify DoD of certain penetrations of protected networks (though not necessarily limited to classified data)
- Sen. Rockefeller issued "cybersecurity" letter to CEOs of Fortune 500 (Sept. 2012)

Legislation: Points of Contention

- Binding regulation or voluntary information-sharing?
- Lead agency: DHS or DoD/NSA?
- Scope of lead agency's responsibility?
- Implications of information-sharing?
  - Antitrust issues
  - Exposure of confidential business information
- Scope of exemption from liability
  - Punitive damages?
  - Privacy?
  - Back door for government surveillance?
- Protection of intellectual property?
- What is "critical infrastructure"?
  - Includes tech firms and government contractors?

White House Initiatives on Cybersecurity

- Draft Executive Order would authorize DHS to promote coordination for private critical infrastructure resources
  - Classified Presidential Policy Directive 20 (signed Oct. 2012) sets new cybersecurity standards for federal agencies
- Comprehensive National Cybersecurity Initiative (CNCI)
  - First established by President Bush in 2008
  - DHS, OMB, NSA: defense against network intrusion; counterintelligence, education, coordination, R&D
  - U.S. Cybersecurity Coordinator: Michael Daniel
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
    - Help create secure online identities to enhance confidence in online transactions
  - National Initiative for Cybersecurity Education (NICE)
    - Improve cyber knowledge and behavior

Defense Department on Cybersecurity

- DoD Strategy
  - Treat cyberspace as an operational domain; Employ new defense operating concepts; Partner with the public and private sector
  - Build international partnerships
  - "[R]ecent events have shown that a purely voluntary and market driven system is not sufficient" to protect critical infrastructure (Gen. Keith Alexander, Head of Cyber Command in a letter to Sen. McCain)
- U.S. Cyber Command
  - Hillary Clinton confirms (5/25): US cyber experts hacked Al Qaeda websites in Yemen and substituted material that bragged about killing Americans with information about civilians killed in terrorist strikes
- DoD Interim final rule to establish voluntary information-sharing with defense industrial base (DIB) companies
- DoD to issue network penetration reporting rules under FY13 National Defense Authorization Act

DHS on Cybersecurity

- Office of Cybersecurity and Communications (CS&C)
  - Common operating picture for cyber and communications across public and private sectors
  - National Cyber Security Division (NSCD)
    - Maintain the **National Cyberspace Response System** and establish a cyber-risk management program for critical infrastructure
      - US Computer Emergency Readiness Team (US-CERT)
        - » Assist operators of agency information systems; inform about threats and vulnerabilities; analyze data incidents
        - » Einstein 1 (network flow monitor); 2 (intrusion detection; 3 (intrusion prevention)

FBI, Cyber Division

- **FBI Resources**
  - National Cyber Investigative Joint Task Force
  - Cyber Action Team; 56 field offices with cyber squads
  - Establishing cooperative working relationships with regulatory groups and agencies
  - Provide briefings to employees regarding economic espionage, counterintelligence, APT, etc.
  - InfraGard (public-private partnership to protect critical infrastructure)
- **What the FBI says that it will not do:**
  - Take over your systems
  - Repair your systems
  - Secure your systems
  - Share proprietary information with competitors
  - Provide investigation-related information to the media or shareholders

FBI Visit on APT

- "Advanced Persistent Threat" attack on defense contractor: not detectable through normal scans
- FBI initiated contact to inform re evidence of penetration and possible exfiltration of data
  - Communications to suspected server
- State-sponsored intrusion (no national state attribution)
- Likely cause: spear phishing malware
  - Downloads attack tools
  - Communicates with malware repository
  - Compromise domain controllers; escalate credentials
  - .exe files renamed; file headers show executable nature
  - .rar files used for compression
- Forensic measures: DNS server logging; full packet capture; firewall logs

Managing Cyber Risks

- Participate in industry and private sector initiatives
  - DHS' US CERT Coordination Center (CERT/CC)
  - US Cyber Consequences Unit (US-CCU), non-profit advisory group that works with industry and DHS
  - Information Sharing and Analysis Centers (ISACs)
    - Cooperatives created by critical infrastructure key resource (CI/KR) owners
    - Current ISACs by sector: communications, financial services, electricity, IT, surface transportation, public transit, water, multi-state
    - Goals: risk mitigation, incident response, alert and information-sharing
  - ISAC Council/National Council of ISACs
    - Facilitates interaction among sector-specific ISACs and the government

Managing Cyber Risks -- Cont'd

- Develop cooperative relationship with key regulators for maximum information-sharing
  - Cooperative relationship with DHS/FBI
  - FOIA exemption for cyber risk sharing in new legislation?
    - » May 2012: D.C. Circuit affirmed denial of FOIA request for information from NSA about 2010 cyber attack on Google targeting Chinese human rights activists
- Examine incident response and notification procedures
  - Prepare for involvement of law enforcement/FBI/DHS
  - Public companies need mechanisms to
    - Assess materiality of cybersecurity issues
    - Determine whether post-incident Form 8-K is appropriate
  - Prepare for technical and legal responses

Government Information Sharing

- Employee / customer perceptions
- Fourth Amendment
  - Are corporations becoming agents of the government?
- All-party consent state wiretap laws
- Inter-governmental re-purposing / sharing
  - Potential use in corporate criminal prosecutions
- Privilege and selective waiver
- FOIA

SEC Cybersecurity Guidance

- Corporation Finance guidance issued Oct. 13, 2011
- Cyber attacks:
  - Target theft of financial assets, intellectual property, other sensitive information
  - Customer or business partner data could be implicated
  - Objectives could include disrupting business operations
- Disclosure if cyber-risks "are among the most significant factors that make an investment in the company speculative or risky"
  - Consider frequency of prior incidents and probability and potential harm of future incidents
  - "Specify how each risk affects the registrant"
  - Avoid generic language

SEC Guidance on Cyber Security Disclosures

- Disclosure required if "are among the most significant factors that make an investment in the company speculative or risky."
  - Determine cybersecurity risks based on frequency of prior incidents and probability and potential harm of future incidents
  - "[A]dequately describe the nature of the material risk and specify how each risk affects the registrant," avoiding generic language
  - At least 21 Dow 30 companies discussed cybersecurity or data breaches in their 2011 Form 10-K risk factor disclosures

SEC Cyber-Comment Letters

In 2012, following hack of Amazon's Zappos servers (involving theft of 24 million customer names and e-mails), SEC asked Amazon to "expand [cybersecurity] risk factor to disclose that you have experienced cyber-attacks and breaches" and "to describe [risks of] third-party technology and systems"

- SEC had disagreed with Amazon's view that hack was not significant enough to be covered by SEC Cybersecurity Guidance

Google, AIG, Hartford Financial Services Group, Eastman Chemical, and Quest Diagnostics were also asked by SEC in 2012 to expand cybersecurity disclosures

International Attention to Cybersecurity

- Fundamental difficulties of attribution
- Budapest Convention on Cybercrime
  - Only international treaty addressing computer crimes
  - Inadequate for scale of current threat
- NATO: "Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organization"
  - Adopted at Lisbon summit in 2010
  - Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - White House Report on "International Strategy for Cyberspace"

International Attention to Cybersecurity

- European Union's Council Framework Decision on attacks against information systems
  - Mirrors the Budapest Convention; binding on Member States
- Digital Agenda for Europe
  - Improve the EU's ability to prevent, detect and respond to network and information security incidents
- European Network and Information Security Agency (ENISA)
  - To ensure a "high and effective level of network information security" in the EU extended through 2020 through creation of EU CERT
- Establishment of EU Cybercrime Center with Interpol
  - Netherlands, January 2013
- Member State initiatives
  - France, Germany, Netherlands, UK, etc.

EU on Cybersecurity Cont'd

- EU-US Cooperation on Cybersecurity
  - Challenge: fundamentally different view of privacy leads to different approach on both data protection and cybersecurity
  - EU-US Working Group on Cyber-Security and Cyber-Crime
    - Established in November 2010 to work collaboratively on coordinated responses to:
      - Cyber incident management
      - Public-private partnerships
      - Awareness raising
      - Cybercrime
  - First joint EU-US cybersecurity exercises (defense stress tests) conducted in November 2011

SIDLEY AUSTIN LLP

SIDLEY

Questions?

Alan Charles Raul:	202-736-8477	araul@sidley.com
Edward R. McNicholas:	202-736-8010	emcnicholas@sidley.com
Jeffrey S. Rothstein:	312-853-7260	jrothstein@sidley.com

www.Sidley.com/InfoLaw

This presentation has been prepared by Sidley Austin LLP as of January 11, 2013 for educational and informational purposes only. It does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking personalized advice from professional advisers.

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG HOUSTON LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.