35th Annual Conference on Securities Regulation and Business Law

Are You Prepared for Anonymous? Securities Lawyers Need to Address Cybersecurity Risk

Stephanie Chandler and Steve Jacobs, Jackson Walker L.L.P.
Christopher J. Volkmer, Volkmer Reid Law Firm PLLC

February 8, 2013

JACKSON WALKER L.L.P.
TEXAS BASED. GLOBAL REACH.™

Speakers

Stephanie Chandler, Partner,
Corporate & Securities Section; Chair of Technology Practice Group; Co-Chair of Cybersecurity Practice

Steve Jacobs, Partner
Head of Corporate & Securities Section – San Antonio Office; Co-Chair of Cybersecurity Practice

Christopher J. Volkmer, Partner
Volkmer Reid Law Firm PLLC
Former chair of the Privacy and Data Security Committee of the Business Law Section of the State Bar of Texas

JACKSON WALKER L.L.P.
TEXAS BASED. GLOBAL REACH.™

"Securing cyberspace is one of the most important and urgent challenges of our time."

~Senator Jay Rockefeller, Chairman of the Senate Commerce, Science and Transportation Committee

The Problem

- Attacks are now systemic
- Cyber Incidents can affect any strategic data of the company – customer data or commercial data
- Directors and Officers have a fiduciary duty to protect assets

Carnegie Mellon – CyLab 2012 Report

- Used Forbes Global 2000
- Boards and senior management still not exercising proper governance

Best Management Practice	Regularly	Occasionally	Rarely or Never
Board reviews & approves top-level policies on privacy & IT security risks	23%	28%	42%
Board reviews & approves roles & responsibilities of lead personnel responsible for privacy & IT security	19%	18%	66%
Board reviews & approves annual budgets for privacy & IT security programs	28%	10%	54%
Board regularly receives reports from senior management regarding privacy & IT security risks	38%	34%	25%

Carnegie Mellon – CyLab 2012 Report

- Boards & management pay attention to enterprise risk management (92%)
- Disconnect: Boards & management still do not make privacy and security and IT part of risk management

How Does It Happen?

- Targeted Attack
  - Competitor, crime ring, amateur, state-sponsored
- Intentional Employee Theft
  - E.g. departing employee leaves with data
- Equipment Theft or Loss
  - E.g. stolen or misplaced laptop or flash drive
- Employee Error
  - E.g. Email mistakes, social engineering
- Outsourcer Security Breach

What is the Nature of Risk?

- Evaluating risk of loss from cyber incident
  - Direct costs
  - Third party liability
  - Fines and penalties
  - Reputational risk
- Resnick v. AvMed and Anderson v. Hannaford Bros. circuit court authority
  - Limits types of state law claims
  - Limits types of damages
  - Permits some claims to be pursued

What is the Nature of Risk?

- Class Actions/Consumer Litigation
- State Law Breach of Contract Claims Resulting from Privacy Policy
- Bank/Credit Card Company Breach of Contract (i.e. requirements to maintain PCI DSS compliance)
- Governmental Authorities (AGs & FTC)
- Chargebacks (Credit Card Data)
- Public Relations Harm: State/Federal/International Law Notice Requirements

What Do The State Laws Require?

- Notification Obligations
  - Notification to Customer
  - Notification to Consumer Reporting Agencies
  - Notification to Applicable Local or Statewide Media
  - Potential Exception: Adopt Company Notification Policy
- Penalties/Fines
- Duty to Properly Destroy

- Optional: Provide Credit Monitoring Services to Breach Victims

What Do Federal Laws Require?

- GLBA
- HIPAA
- FTC Act Section 5

The SEC

- Letter to Chairman Schapiro
- Responded in June ’11
- Guidance issued in October ‘11

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

DIVISION OF
CORPORATION FINANCE

May 18, 2012

We have reviewed your filing and have the following comments. In some of our comments, we may ask you to provide us with information so we may better understand your disclosure.

1. We note that none of your risk factors, or other sections of your Form 10-K, specifically address any risks you may face from cyber attacks, such as attempts by third parties to gain access to your systems to compromise sensitive business information, to interrupt your systems or otherwise try to cause harm to your business and operations. In future filings, beginning with your next Form 10-Q, please provide risk factor disclosure describing the cybersecurity risks that you face or tell us why you believe such disclosure is unnecessary. If you have experienced any cyber attacks in the past, please state that fact in any additional risk factor disclosure in order to provide the proper context. Please refer to the Division of Corporation Finance's Disclosure Guidance Topic No. 2 at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm for additional information.

SEC Guidance

- Risk factors (See Appendix – available at www.jw.com)
  - Description of outsourced functions that have material cybersecurity risks;
  - Description of cyber incidents experienced by the registrant that are material, including a description of the costs and consequences; and
  - Description of relevant insurance coverage for cyber incidents.
- MD&A
  - Cost
- Business
  - If there has been an incident
- Legal Proceedings
- Financial Statements
- Effect on Internal Controls (SOX)

What Should Corporate Boards Do?

- CTO/Chief Security Officer – Direct Report (or Report to Audit or Risk Committees)
  - At least annual review of cybersecurity program by the board or a committee
  - Educate the board on Cybersecurity risks and reporting duties
- Disclosure Committees
- Risk Oversight – "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."

What Should Corporate Boards Do?

- Mitigate risk by insurance
  - Prior to the Breach – Hack Insurance/ Cybersecurity Insurance
  - After the Breach
    - CSIdentity
    - Debix
    - Experian Credit Bureau
- Security Audits
  - Document Retention Policies
  - SAS70 Now SOC
    - SOC 1 - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
    - SOC 2 - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and/or Privacy
    - SOC 3 - Trust Services Report

Financial Reports (SSAE 16)

Non-Financial Reporting (AT101)

JACKSON WALKER L.L.P.
TEXAS BASED. GLOBAL REACH.™

FIDUCIARY DUTIES

Questions

Contact

Stephanie Chandler	210.978.7704	schandler@jw.com
Steve Jacobs	210.978.7727	sjacobs@jw.com
Chris Volkmer	214.336.0270	chris@volkmer-reid.com

JW | JACKSON WALKER L.L.P.
TEXAS BASED. GLOBAL REACH.™

Appendix
Sample Risk Factor

Security breaches and other disruptions could compromise our information and expose us to liability, which would cause our business and reputation to suffer.

[In the ordinary course of our business, we/We] [collect and] store sensitive data, including intellectual property, our proprietary business information and that of our customers, [suppliers and business partners,] and personally identifiable information of our [customers and] employees, in our data centers and on our networks. The secure [processing,] maintenance [and transmission] of this information is critical to our operations [and business strategy]. Despite our security measures, our information technology and infrastructure may be vulnerable to attacks by hackers or breached due to employee error, malfeasance or other disruptions. Any such breach could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could result in legal claims or proceedings, [liability under laws that protect the privacy of personal information,] [and regulatory penalties,] [disrupt our operations [and the services we provide to customers],] [and] damage our reputation, [and cause a loss of confidence in our products and services], which could adversely affect our [business/operating margins, revenues and competitive position].

Source: PLC Securities

Examples of Risk Factors

- ***Google Inc. Annual Report on Form 10-K for the fiscal year ended December 31, 2011*.**
- ***Citigroup Inc. Annual Report on Form 10-K for the fiscal year ended December 31, 2011*.**
- ***Lockheed Martin Corporation Annual Report on Form 10-K for the fiscal year ended December 31, 2011*.**
- ***EMC Corporation Annual Report on Form 10-K for the fiscal year ended December 31, 2011*.**
- ***The Coca-Cola Company Annual Report on Form 10-K for the fiscal year ended December 31, 2011*.**
- ***Electronic Arts Inc. Quarterly Report on Form 10-Q for the period ended December 31, 2011*.**
- ***ATA Inc. Annual Report on Form 20-F for the fiscal year ended March 31, 2011*.**
- ***CoreLogic, Inc. Annual Report on Form 10-K for the fiscal year ended December 31, 2011*.**
- ***Alliance Data Systems Corporation Annual Report on Form 10-K for the fiscal year ended December 31, 2011*.**

Sample Risk Factor

[ADDITIONAL RISK FACTOR DISCLOSURE FOR COMPANIES THAT HAVE EXPERIENCED A SECURITY BREACH]

[In [DATE] [[our computer network/our website] suffered [cyber attacks/unauthorized intrusions] in which [customer data/proprietary business information] was accessed [and stolen]/[DESCRIBE SPECIFICS OF CYBER ATTACK OR OTHER BREACH]]. Following the[se] attack[s], we have taken [additional] steps designed to improve the security of our networks and computer systems. Despite these defensive measures, there can be no assurance that we have adequately protected our information or that we will not experience future violations.]

Source: PLC Securities

Examples of Risk Factors

Examples of description of previous attacks or breaches:

- ***Sony Corporation Annual Report on Form 20-F for the fiscal year ended March 30, 2011*.**
- ***The TJX Companies, Inc. Annual Report on Form 10-K for the fiscal year ended January 29, 2011*.**
- ***The NASDAQ OMX Group, Inc. Annual Report on Form 10-K for the fiscal year ended December 31, 2011*.**

Examples of Risk Factors

- ✓ **Consider Describing Your Preventative Actions**
- ✓ **Examples:**
- ***Microsoft Corporation's Quarterly Report on Form 10-Q for the period ended December 31, 2011*.**
- ***Adobe Systems Incorporated Annual Report on Form 10-K for the fiscal year ended December 2, 2011*.**

JW | JACKSON WALKER L.L.P.
TEXAS BASED. GLOBAL REACH.™