WOODRUFF SAWYER & COMPANY

A WS&CO. ARTICLE

Insurance Services | Risk Management | Employee Benefits

June 2013

Cyber-Threats: The Board's Role and Some Useful Questions

By Lauri Floresca[1] & Priya Cherian Huskins[2]

WHAT IS THE BOARD'S ROLE WHEN IT COMES TO HANDLING CYBER-THREATS?

Board members are being advised to assess cyber-security exposures at their companies. But how is a board member to tackle this topic when it is clearly management's job to handle operational issues like cyber-security? And does the board have the knowledge required to conduct such an assessment?

The board's role, as always, is to ask the right questions, help set priorities, demand accountability, and serve as a strategic resource. A process-oriented, systematic approach to surfacing cyber-threat issues is consistent with this role.

Recognizing that most management teams will have already taken active steps to scope and address cyber-risk, this list of questions can serve as a starting point for a board in its evaluation of that work. The questions are categorized into three areas of inquiry: the risk assessment process, inventory of vulnerable assets, and risk mitigation and/or transfer.

CYBER-THREATS: KEY QUESTIONS FOR BOARDS OF DIRECTORS

Risk Assessment Process

- What is the most likely source of a cyber-threat for us:
  - Competitor?
  - Rogue employee?
  - Criminal individual or enterprise motivated by greed?
  - Foreign government, especially if interested in our IP?
- Who is responsible for cyber security at the company (CIO alone? GC? Others?)
- Has a cyber risk assessment been done?
  - Who did the assessment?
  - Was "social engineering" an element of the assessment?
  - What did forensic IT learn from our last breach?
- Where is our data physically located? What are our plans should we lose our main servers?
- Do we have a data breach response plan in place?
  - Has it been tested?
  - Do we have a PR plan ready to go?
- What training do we currently provide our employees?
  - Password management, public wifi use, social hacking, etc.
- What is our board process to assess cyber liability?
  - Who are the directors with the competence to address the issues?
  - Has an ad hoc committee been formed to address the issues in a systematic way?

Inventory of Vulnerable Assets

- What kind of data do we have?
  - What is mission critical (e.g. IP, strategic plans, competitively sensitive information)?
  - What can take longer to recover/restore?
  - What cannot be restored once taken?
- Concerning customer/user data

(continued on page 2)

[1] *Lauri Floresca is a partner at Woodruff-Sawyer and an expert in the disciplines of both D&O insurance and Cyberliablity insurance. She can be reached at lfloresca@wsandco.com or 415.402.6523.*

[2] *Priya Cherian Huskins is a partner at Woodruff-Sawyer and an expert on D&O liability and its mitigation using insurance and non-insurance solutions. She can be reached at phuskins@wsandco.com or 415.402.6527.*

  - What kind of data do we collect/store from our customers/users?
    - Names, addresses, email addresses
    - Password and login ID
    - Credit cards
    - Social security numbers
    - Financial records or health information
  - How many individual consumer accounts/records do we have?
- Do we use third party vendors to store data or process information?

Risk Mitigation and/or Transfer

- Do we encrypt customer data? To what standard? At rest and in transit?
- Do we purge old data?
- How are the evolving legal requirements concerning collection, storage, and notification-in-case-of-breach being monitored and applied?
- Contractual protections:
  - Do we limit liability in our standard enterprise customer agreements? How often do we deviate from our "standard" agreement?
  - For consumer/small business customers, do our agreements include a mandatory arbitration provision with a class action waiver?
  - What indemnity rights or limitations on liability exist in our contracts with payment processors, cloud providers, or other outside IT vendors?
- Do we allow third parties to advertise on our websites? If so, are they obligated to indemnify the company in the event of a suit regarding their data collection practices?
- Do we have a viable insurance solution/ are we transferring risk in the following categories?
  - Direct costs associated with a cyber security breach including forensic IT, notification costs, and credit monitoring
  - Fines and penalties from regulatory bodies
  - Lawsuits by customers/users
  - Loss of revenue related to a cyber security failure
  - Reputational risk
- What metrics have we used to establish appropriate limits in these categories?

Questions? Comments?

Please contact your Woodruff-Sawyer account executive, or the authors, at 415.391.2141.

Woodruff-Sawyer is one of the largest independent insurance brokerage firms in the nation, and is an active partner of International Benefits Network and Assurex Global. For over 90 years, Woodruff-Sawyer has been partnering with clients to implement and manage cost-effective and innovative insurance, employee benefits and risk management solutions, both nationally and abroad. Woodruff-Sawyer is headquartered in San Francisco.

For general information, call 415.391.2141 or visit www.wsandco.com.