MORRISON FOERSTER

# CYBERSECURITY AND THE BOARD

Cybersecurity has rapidly emerged as a top-of-mind issue for many Boards of Directors in the wake of recent large-scale data security incidents. Boards are engaging with management teams in new ways in order to assess cybersecurity risks and the company's readiness to respond to emerging threats.

These threats have placed additional pressure on Boards in part due to the level of attention and adverse scrutiny directed at other data security incidents. This includes scrutiny from shareholder advisory service firms as well as a number of government agencies, including the FTC, the SEC, and state Attorneys General, who routinely investigate data security incidents. While the "business judgment rule" can be expected in most circumstances to provide protection to the Board in the event of shareholder litigation regarding data security issues, a careful review and assessment of the company's level of preparedness for cybersecurity risks is a helpful step in mitigating risks to the business.

Although there is no simple solution to this set of issues, there are three broad topics that many Boards of Directors are examining as they review and assess these issues:

- how important cybersecurity is to the company;
- what steps the company has taken to evaluate and mitigate cybersecurity risks; and
- what public disclosures the company has made.

## How Important Is Cybersecurity to Your Company?

- What is the scope of information regarding individuals—customers, vendors, or employees?
  - Almost every company has some personal information regarding individuals.
  - In general, companies which are consumer facing or for whom information is the primary asset, as well as those with large numbers of employees, have more pronounced cybersecurity risk.
- How important is information security to your brand?
  - If your company had a cybersecurity incident, would it make it more difficult to sell your products or services?
  - Is maintaining customer trust regarding information important to your business?
  - If the answer to any of these questions is "yes," then your company has a higher cybersecurity risk.
- Does your company have valuable or sensitive proprietary data that someone might seek to steal?
  - While theft of personal information and credit cards is in the news, there is a great deal of other cybercrime, including attacks directed at proprietary information, trade secrets, business processes, and other corporate assets


continued on page 2

including cash.

  - Whether or not your company is consumer facing, if your organization has sensitive proprietary information, it may be a more attractive target to cybercriminals than you think.

- Is your company "critical infrastructure," or are you a supplier/vendor for the government, or for critical infrastructure?
  - Companies deemed to be critical infrastructure or that provide services to the government face special considerations.
  - For example, these businesses are likely to be regulated on cybersecurity matters sooner rather than later.

## Has Your Company Taken Steps to Evaluate, Mitigate, and Govern the Risks?

- What organizational structures exist to measure, govern, and assess data and information risk and how are threat assessments managed and reported?
  - Companies with cybersecurity risk need to understand the risks they face and should consider formalized governance structures or processes to measure, assess and mitigate that risk.

- Is responsibility for all aspects of protecting your company's information assets allocated appropriately?
  - Having a clear chain of command and a specific allocation of duties for those charged with information protection can both mitigate cybersecurity risks and prepare the organization better to respond to a security incident.
  - Has a comprehensive risk assessment regarding information security been completed recently and what is the status of addressing issues identified in such a risk assessment?

— A good place to start a risk assessment is to:
  - » complete a high level data inventory of the company's information assets so that you have an understanding of what information you have and generally where it is located; and
  - » do a thorough review of policies and procedures to ensure that they comply with the relevant data security laws and are consistent with industry best practice.

- Has the company assessed the impact of global privacy and data security laws on the business?
  - While there a number of different U.S. laws dealing with cybersecurity and data protection, there are also more than 90 other countries that have data protection laws.
  - If your company is operating outside of the U.S. it is important to take the global laws into account when designing a cybersecurity program.

- Does the company have an incident response plan, and are the appropriate business leaders identified in it?
  - For many companies, it is not a question of if you will have a security incident so much as when.
  - Having a clear written incident response plan can help companies effectively respond to a security incident.

- Have the company's security processes and systems been reviewed by a third-party assessor?
  - Third-party review of cybersecurity readiness can be a crucial factor in defending the company after a security incident as well as helping a company to take reasonable steps to prepare for and defend against a cyberattack.
  - Consider the following kinds of questions:
    - » Does the company have a Security Operations Center, or other similar group in the company, and if so, have its activities been reviewed by a third-party to ensure they are adequate?
    - » Has the level of penetration testing, software patching, and other similar activities been reviewed by a third-party to ensure it is adequate for your company?


continued on page 3

» Has the company benchmarked its cybersecurity risk posture against other similar businesses?

- Many Boards of Directors are taking additional steps in order to establish that they are exercising appropriate oversight of cybersecurity.
  - One crucial question that may be asked in the wake of significant information security breaches is "was the Board engaged?"
  - To assure that you will be able to answer that question with confidence, consider: when was the last time the Audit Committee or other responsible committee of the Board received a report regarding information security and when was the last time the Board received such a report?
- Does the company carry insurance that covers cyber risk?
  - Cyber risk insurance is becoming much more common in recent years and is one tool that can be used to help the company to manage risk.
- What Public Disclosures Has the Company Made?
  - Do the company's public disclosures on information risk adequately describe its current risk posture?
  - In October 2011, the SEC's Division of Corporation Finance issued guidance regarding disclosure obligations related to cybersecurity risks and cyber incidents. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
  - Generally speaking, that guidance discourages "boilerplate" disclosures related to cybersecurity issues, and outlines issues to consider when a company is drafting the risk factors, MD&A, business description, legal proceedings, and financial statement portions of its public filings.
  - The Chair of the SEC, along with various staff members, has been publicly asking questions about whether companies are being sufficiently transparent in their disclosures about cybersecurity and cyber incidents.
  - In addition, Target has publicly disclosed that it is under investigation by the SEC for its disclosures related to cybersecurity.
  - Closely reviewing the company's data security policies, prior cyber incidents, and material information concerning cybersecurity risks in connection with drafting periodic filings is important as long as this issue is a priority for the SEC and its staff.
- Assess the company's internal and external privacy and information security policies and statements to confirm they appropriately and adequately describe its information practices.
  - Read the publicly facing privacy statements on the company's website or in the literature the company provides to customers.
  - Ask whether it is consistent with the company's actual practices and what methods are used to ensure that the company upholds the promises that it makes.

## For more information on these issues, please contact:


**Miriam Wugmeister**
(212) 506-7213
mwugmeister@mofo.com

**Nathan Taylor**
(202) 778-1644
ndtaylor@mofo.com

**Kristen Mathews**
(212) 336-4038
kmathews@mofo.com

**Alex van der Wolk**
Brussels 32 23407369
London 44 (20) 79204074
avanderwolk@mofo.com

**Alex Iftimie**
(415) 268-7673
aiftimie@mofo.com

**Robert S. Litt**
(202) 887-1588
rlitt@mofo.com