FOLEY

FOLEY & LARDNER LLP

Board Oversight of Data Privacy and Security

2007 NATIONAL DIRECTORS INSTITUTE

BOARD OVERSIGHT OF DATA PRIVACY AND SECURITY

The seemingly simple obligation to keep confidential information from becoming public is a growing concern for businesses and their customers. Businesses collect and store ever-increasing amounts of data regarding customers, suppliers, employees and products. The collection of this information is quiet, but security failures are announced loudly, with news headlines and lawsuits.

Because of the potentially devastating consequences that security failures can have for a business, the entire enterprise must make a commitment towards effective data protection and must make itself knowledgeable about the risks and values in its information resources. Data protection has strategic importance to the modern enterprise and cannot be left for the information technology professionals alone. A board of directors must have the knowledge and structure necessary to ask the right questions, provide appropriate guidance, and establish effective oversight.

At Foley's sixth annual National Directors Institute on March 8, 2007 in Chicago, "Board Oversight of Data Privacy and Security" was a featured breakout session. The panel was moderated by Mark Foley, partner, Foley & Lardner LLP, and included Patrick Donnelly, managing director, Aon Corporation's Financial Services Group; Joe Boucher, partner and founding shareholder, Neider & Boucher, S.C.; and Rick Siebenaler, principal, Deloitte & Touche LLP and former Chief Scientist for the National Computer Security Center.

The Importance of Data Privacy and Security

Data privacy and security revolve around three fundamental issues: confidentiality, integrity, and availability.

Confidentiality refers to controlling information to the extent required by law, contract, or business purpose. Some need for confidentiality will exist whether the information is customer data, intellectual property of the company, or third party data. What information a company must keep confidential and what level of security to apply are highly individualized analyses, and will necessarily vary significantly for each company.

Integrity refers to the quality of data — ensuring that company data and information systems are accurate, complete, and up to date. Integrity means protecting data from modification, not only by malicious actors such as competitors, viruses, hackers, or others who might attempt to modify your data or take control of your systems to attack other networks, but also by well-meaning, but ill-informed, employees.

Availability means reliably providing access to corporate data to those who need it, when and where they need it. It includes both the ability to prevent attacks that can limit access to critical business systems, and also the ability to recover from those attacks and from physical disruptions such as floods and storms. A company must provide sufficient data confidentiality, integrity, and availability to its customers and employees; none of those can be provided without adequate security.

The Board's Role

A board plays a vital role in overseeing data privacy and security. Companies must address data privacy and security at the board level, for many reasons.

First, the board's core duty — the fiduciary duty of care and loyalty — necessarily involves a paramount duty to protect the company's most important assets. In many cases, a company's most valuable assets are no longer physical things, but rather intangible information. These assets include the company's reputation, its trade secrets, business plans, pricing information, private financial data, and customer and contract information. As more of a company's value flows from these assets, board oversight becomes increasingly important.

Second, effective security for these assets requires enterprise-wide coordination, interaction, and enforcement of policies. There are a host of legal obligations of which the company must be aware; the complexity of these obligations increases with the number of different domestic and international jurisdictions in which the company operates.

Third, information technology requires substantial funds, and a board's disinterest can lead to squandering of the funds invested. A recent study showed that over 60 percent of major information technology initiatives fail to achieve their major goals or are abandoned entirely. Examples of such failures abound in the news, including a distribution system shutdown at a candy company which led to major supply disruptions in the months leading up to Halloween and a drop in stock price, and a large oil company, which had to postpone installation of a worldwide enterprise resource planning system because it failed to address European Union (EU) data privacy requirements.

Fourth, board oversight of data security is critical for instilling a culture of privacy and security; without it, any policy initiative will devolve into non-compliance.

Fifth, the rules and priorities must be enforced to prevent security failures. Without strong board support, compliance will dwindle.

Sixth, any security failures are likely to become public. Every day, it seems, brings another story in the news about theft of laptop computers, employee theft of information, and other security breaches which cause embarrassment and scandal. Recent examples include a state department of revenue mailing tax forms with the addressee's social security number on the outside of the envelope, and a federal agency whose security was breached exposing personal information of more than 40 million Americans, including scores of members of Congress.

Finally, the risks to the company from inadequate data protection are real and significant. Companies with public data security breaches have suffered immeasurable loss of reputation, major customer defections, civil fines, stock price drops, criminal prosecutions, and the imposition of long term regulatory oversight.

While some wonder about the level and frequency of "sponsorship" of data security at the board level, the experiences run the gamut from the board remaining completely disengaged at one extreme, to the chief security officer reporting to the board at every meeting. Businesses maintaining a higher degree of information intensity tend to give

higher attention to this issue, but a minimum level of involvement by the board increasingly is expected.

Controlling Risk

The principal types of risk that can arise from inadequate board supervision of data privacy and security can best be summarized as regulatory, litigation, and enterprise risk.

Regulatory risk is the danger of regulatory action befalling the company as a result of failure to comply with laws applicable to specific types of data, industries or practices. It can arise from unauthorized disclosures of information, from failure to comply with stated policies or failure to implement appropriate security. Regulatory risk also can come from failure to comply with international data transfer rules.

Litigation risk is the risk of a suit for damages against the company. Such suits can take the form of claims by data subjects for wrongful disclosure or use of their data, claims from business partners for breach of data handling agreements, from employees for harassment, discrimination, or invasion of privacy, or by shareholders for loss of stock market valuation. Because of the immediacy of a board's duties to shareholders, and the ready willingness of securities class action lawyers, these suits provide the most likely litigation threat.

Enterprise risk, or risk to the company's value as a result of poor privacy and security practices, presents the gravest threat. The damage done to a company's reputation from an article in the financial press can be much greater than that from a lawsuit, and longer lasting. Enterprise risk manifests itself in the loss of customer confidence and contracts, loss of trade secrets, inability to access important information, disruption of business, and loss of stock market value, in addition to antitrust fines, penalties and damages.

Managing the regulatory, litigation, and enterprise risks arising out of inadequate data protection systems requires a board to understand the data and how it is processed, and the systems involved and how changes to those systems create new risks. It requires a company to understand its legal and contractual obligations, and the regulations applicable, which vary substantially among jurisdictions. In the EU, for example, the standard regarding ownership of a consumer's personal data is that the customer owns it; in the United States, the company, not the consumer, typically owns the data.

Key events — such as outsourcing, introduction of new information technology hardware and software, major business process changes, and mergers and acquisitions — often create new data privacy and security risks for a company. Enterprise Risk Planning systems, for example, can become mega-repositories for data, whose implementation requires reassessment of data security issues.

Outsourcing of information technology functions is a growing practice for many companies, but it is advisable for the in-house legal department to hold on to audit rights, including SAS 70 audits of internal controls over information technology and related processes. The company must not only hold onto those audit rights, but it is critical for the company to exercise them regularly. In addition, the company's security personnel should be embedded in the team that makes contracts for any such outsourcing. The

reason for such diligence is simple: a hacker needs to find only one weak link in a company's defenses, while the company must find them all. Disclosures can expose companies to massive enterprise risk, and companies have seen huge losses of intellectual property, bankruptcies, and research and development — some totaling more than $100 million overnight. Furthermore, any other companies that rely on the breaching company also suffer in a breach.

The frequent occurrence of news stories about data security breaches has not made the public immune to their impact, even though people may seem less shocked by such breaches than in the past. Even if those whose data has been stolen experienced no real harm from the thefts, the risk of identity theft has increased and may not yet be fully realized. Furthermore, thousands of documented attempts to gain unauthorized access to data go unreported in the press each year. Data theft is a young process and the evidence from thefts that have already occurred can surface at a later date. Because of this uncertainty, companies need to question whether notification laws apply to data thefts, whether to offer credit monitoring, and what reporting obligations may apply.

Insurance

Data security needs have driven changes in insurance. Traditional insurance was written for a world of physical or tangible assets. That world no longer exists. The things that create the most value, wealth and competitive advantage in today's economy are mostly non-physical; data and intellectual property are not tangible assets. Traditional insurance was not intended or priced to cover data security risks, and early policies provided little coverage, insuring only a limited number of events. For example, data were not tangible property traditionally covered by comprehensive general liability (CGL) policies, confusion existed over whether non-physical perils triggered Business Interruption/Extra Expense policies, and traditional CGL policies contained only limited coverage for intellectual property, advertising injury, or privacy.

Despite the limitations in early practice, as more money has flowed into cyber-risk policies, newer policies have emerged which provide broader coverage with a wider array of triggering events and better assessment of data security and privacy risks. As a result, recent iterations of information security and privacy coverage must be explored as part of a comprehensive risk management strategy. Policies have evolved to cover first-party loss, network-related business interruption/extra expense loss, and intangible asset damage. More recent policies also include coverage for accidental damage/destruction and administrative or operational error, and feature improved valuation of loss models, lower time-based retentions, and contingent coverage that contemplates significant business process and information technology outsourcing relationships. Insurance should always be the last step in any board assessment of data security and privacy; a company must thoroughly understand its risks before insuring against them. If the board does not understand its risks, trying to insure against them can be difficult, and expensive.

Best Practices

One size does not fit all when it comes to data privacy and security; a board of directors must adopt the practices that best fit the company. There are several best practices that every board should incorporate, including:

Establishing clear responsibility for data security. The board should place responsibility with a committee or with a designated officer; it could be the CEO, CIO, or Chief Security Officer (CSO). The board also should create an audit committee with adequate substantive knowledge. If the board creates a technology committee, the people on the committee should be comfortable talking about the issues relating to technology and data protection.

Developing internal and external audit procedures for data security. The process should include gap analysis and secret testing of security — including staged attacks, such as denial of service attacks, Trojan horses, DNS poisoning, worms, send mail attacks, and others. The head of data security, or the CEO, should be required to report issues and progress to the technology committee.

Prospectively developing effective crisis management procedures. To ensure the privacy and security of data, a company must regularly assess its actual data collection, use, and dissemination practices, and conduct regulatory and contractual gap analyses. A company must establish policies to accurately describe actual practices, establish privacy security practices to enforce controls, and establish change control and breach response procedures. A company must audit and test, and finally, assess whether to insure against the remaining risks. These practices must be in place before any problems arise; the aftermath of a consumer or customer data leak is the worst time to discuss implementation of a crisis management plan with the board of directors.

Staffing internally for data security is an important concern. It is critical for at least one top executive or board member to understand data flows, and to obtain legal input regarding compliance, although no solution fits every company. For some companies, a data security team is the best solution, while for others the best solution is for the responsibility to reside with the head of human resources, CIO, or Chief Technology Officer (CTO). For others, the best solution may be a cross-functional team and an executive who can act as a point person or champion. Each company is different, and decisions about staffing and cost issues depend largely on the systems and infrastructure already in place.

Any board of directors must continually test its management on data security issues. The board should question the CEO, or other person selected to have top level responsibility for data protection, on this topic – repeatedly – as a part of its normal activities. The company must also update its responses when major events arise, such as the acquisition of a new business, or as an existing business acquires new uses for data. More detailed questions should be asked by the CEO or the board's technology subcommittee to help drill down into those areas that may require deeper analysis and understanding.

For More Information

For more information on this session or the sixth annual National Directors Institute, visit Foley.com/ndi2007 or contact the panelists directly.

Joseph Boucher
Neider & Boucher, S.C.
jboucher@neiderboucher.com

Patrick Donnelly
Aon Financial Services Group
Patrick_donnelly@ars.aon.com

Mark Foley
Foley & Lardner LLP
mfoley@foley.com

Rick Siebenaler
Deloitte & Touche LLP
rsiebenaler@deloitte.com

2007 National Directors Institute Sponsors

Foley proudly recognizes the 2007 National Directors Institute sponsors: UBS, Aon, Korn/Ferry International, Deloitte, RR Donnelley, D. F. King, Ashton Partners, Boardroom Bound, Chicagoland Chamber of Commerce, NASDAQ, NYSE and Springboard Enterprises. The support we receive from our sponsors is crucial to the development of the program and we thank them for their efforts in once again making NDI a huge success.

Save the date! The 7th Annual National Directors Institute will be held on March 6, 2008 in Chicago. Learn more at Foley.com/ndi.