Guest Contributors: Who is Mining the Store? Corporate Governance and Data Privacy/Security Issues

GUEST CONTRIBUTOR POST: *Kevin F. Brady is a litigation partner and chair of the Business Law Group and the Information Security, Electronic Discovery and Records Management Group of the Wilmington, Del., office of Connolly Bove Lodge & Hutz LLP. Francis G.X. Pileggi is the founding partner of the Wilmington office of Fox Rothschild LLP. He started a blog at www.delawarelitigation.com that summarizes all the key decisions on corporate and commercial law from Delaware's Court of Chancery and Supreme Court. Mr. Brady is a frequent contributor to the blog. This post is exclusive to The Conference Board Governance Center.*

By Kevin F. Brady and Francis G.X. Pileggi

Managing electronic data, especially data privacy and data security concerns, have been elevated to C-level attention and a regular slot on the board's agenda due to the substantial increase in costs and risks arising from these issues. Chief Information Officers, Chief Privacy Officers and Chief Security Officers are constantly worrying about who might be "mining" the company's e-data looking to steal trade secret, patent or personal information.

The risk of losing millions of dollars of important information is very real. It seems like not a day goes by without a major security breach being announced in the media.

According to the Privacy Rights Clearing House, since January 2005 more than 510 million records have been *reported* as having been breached in some form from private and public companies (large and small), colleges and universities, state and federal governments. [See list.]. Even the Dalai Lama is not immune from hackers mining data on his servers. [See March 2009 New York Times article, "*Vast Spy System Loots Computers in 103 Countries.*"].

More than 40 states have laws that require the custodian of the data that was lost to notify the individuals whose data was lost. Some states have enacted laws which have broad reach beyond their borders to protect their citizens' data with heavy fines for violations. For example, there is a Massachusetts law (201 CMR 17.00) that applies to any company which holds personal information of a Massachusetts resident (with no restriction as to where the holder of the information is located) and it carries a fine of $5,000 per violation and per record lost. Companies also must be concerned about compliance with a number of federal laws such as the Sarbanes-Oxley Act, HIPPA, Gramm–Leach–Bliley Act and PCI Data Security Act.

BOARD LEVEL RESPONSIBILITY

When companies implement a records management policy, they typically include data privacy and security as part of the data governance mandate. Effective compliance with internal records management policies requires collaboration and institutional commitment from the top down. Why should the board be concerned? Could it be a breach of a fiduciary duty if protective measures are not in place to ensure a high degree of security for corporate records? Case law *suggests* but does not yet mandate that corporate officers and directors' fiduciary duties extend to managing the company's electronic information. However, directors and officers are responsible for overseeing the safety of corporate assets including electronic information.

Directors and officers in exercising their fiduciary duties of care and loyalty must establish policies and procedures to protect the company's business-critical e-information. The board also needs to question management regarding, among other things: (i) the implementation of organizational measures such as internal management of critical information; (ii) procedures for implementing, educating, enforcing, as well as assessing and updating the policies; (iii) plans for mitigation and effective responses should a breach occur; and (iv) audit policies and procedures with consequences for non-compliance.

Failure to provide appropriate data governance can quickly become a crisis, and the failure to appreciate that technology is changing at an increasingly rapid pace with companies (and their lawyers) struggling to catch up, can compound the problem. Two new areas on the "technology horizon" – cloud computing and social networking sites – are especially challenging for companies.

CLOUD COMPUTING AND OUTSOURCING THE IT PROCESS

"Cloud computing" or the "virtualization of the computing process" is being touted as the future of electronic records management because of the potential for significant cost savings in the short and long term. Cloud computing helps companies eliminate the capital investment needed for applications (software and hardware) to perform the computing because data is stored "in the cloud" (on the internet) on information systems owned and operated by third parties.

Cloud computing greatly reduces the large capital expenses associated with electronic data management – software, hardware and IT personnel services.

However, security and data privacy are critical concerns. While the customer legally owns its data in the cloud, it does not have the level of "control" over its data that it would if the data was handled in the traditional sense – stored at the customer's facilities within the customer's infrastructure.

The key component to the successful implementation of cloud computing is the agreement between the customer and the third-party service provider. To avoid costly mistakes, a customer must craft an agreement that addresses anticipated problems such as: (i) where will the data reside and will it be backed up? (ii) who will have access to the data and will there be different levels of access? (iii) who will supervise the project and will there be monitoring and auditing of the policies and procedures? and (iv) what security measures are in place?

SOCIAL NETWORKING — NOW ACCEPTED IN THE BEDROOM AND THE BOARDROOM

Social networking Web sites have recently become a very popular method of communication not only in employees' private lives but also in the business environment. Sites like Facebook, LinkedIn, and Twitter allow users to create online profiles where they can choose to display their friends and interact with the

online community. Given the breadth of these online communities and the wealth of personal information they contain, companies have started using social networking sites to enhance many corporate initiatives such as marketing and recruiting. In litigation, lawyers are starting to direct formal discovery requests to companies for information their employees might have placed on social networking sites.

Just as companies and business litigators face discovery preservation issues with company websites, email correspondence and electronic information, so too must companies be prepared to preserve and produce information on social networking websites they control in order to prepare for potential litigation.

In addition, companies should be wary of what their employees are posting on the internet, especially when discussing the company or its competitors, as the employer may be held liable and/or face significant problems. For example, in 2007, it was revealed that a CEO of a large publicly-held corporation was using a pseudonym and was posting disparaging remarks about a competitor. The discovery prompted an SEC investigation and raised some interesting and novel SEC-related issues.