PUBLICATION

Information Security Management and Business Valuation

August 25, 2008

Information security is a concern for almost all aspects of business and tax compliance and planning functions within a business organization are certainly not immune from these concerns. For instance, when performing a valuation of a business, determining potential liabilities on a balance sheet or conducting due diligence in transactions, significant consideration should be given to direct and indirect costs involved in complying with or failing to fully comply with: federal, state and international privacy laws and regulations; contractual privacy requirements; customer and shareholder dictates involving information security management[1]; identity theft prevention[2]; and IT governance[3]. The failure to properly consider such costs could have significant and/or catastrophic results to organizations. Conversely, for those organizations that do understand their responsibilities and implement plans to integrate legal, contractual and marketplace requirements into a framework that leverages these requirements, a valuation premium could be in order.

Senior management, particularly of those organizations that collect sensitive consumer information, who do not appreciate their significant oversight responsibilities and the need to address information security management and identity theft prevention first at the governance level and next at the operations level, may find themselves in the unenviable position of having to report security breaches to customers, regulators and shareholders. Thousands of organizations, from large financial institutions and government entities to mid and small size retailers and service providers have reported breaches. A few of the well publicized incidents include those of:

- TJX Companies, Inc., parent company of retailer T.J. Maxx, which has written off or borne expenses in excess of $100 million because of security breaches resulting in the compromise of, by many estimates, over 100 million payment card numbers;
- ChoicePoint, Inc., one of the largest data brokers in the U.S., as a result of selling credit data of over 145,000 consumers to identity thieves, lost major customers, was involved in costly litigation and enforcement actions (including $10 million in civil penalties and $5 million in consumer redress) and has had its name attached to resulting state security breach notification laws that have now been enacted in most states; and
- The former CardSystems Solutions, Inc., a company that provided merchants with authorization services for credit and debit card purchases, which was acquired by another company after a breach to its IT systems and exposure of 40 million credit card numbers to hackers, resulting in millions of dollars of fraudulent purchases.

While the costs of compliance with the requisite laws and regulations, when viewed strictly as compliance, may be significant, the failure to do so can be significant and/or catastrophic. On the other hand, compliance expenditures can be turned into a distinct competitive advantage when aligned with business processes and IT optimization.

So what steps should be taken by organizations?

1. Involve legal advisors in the process. Lawyers are in a position to credibly translate legal, contractual and even marketplace requirements into actionable and legally compliant policies and procedures that set the tone and provide the umbrella for the next level of policies and procedures involving the legal, human resources, IT, marketing, public relations, internal audit and other departments. (Pre-

planning for security incidents, litigation preparedness incorporating electronic discovery requirements and incorporation of IT and information security management standards, frameworks and controls can greatly reduce exposure to the direct and indirect costs surrounding security breaches).

2. Understand the inter-relationship of legal, contractual and marketplace requirements and how they may be integrated into a variety of different IT and information security management frameworks and best practices.
3. Align these frameworks and best practices with business best practices and quality improvement criteria such as the Malcolm Baldrige National Quality Award, Six Sigma, Lean Manufacturing, and Balanced Score Card and in compliance with industry standards (e.g., QS 9000, ISO 9001/2000, ISO 14000, ISO 17799/2005 (27002), ISO 20000).
4. Give the information security management program time to work and understand resource capacity. Much of the value of these programs and their success centers on people – employees understanding their roles and responsibilities. It is neither easy nor necessarily quickly accomplished, because management's commitment to information security management must be translated into actionable steps, and all stakeholders, most importantly employees, must understand their information security management roles and responsibilities.
5. Consider having a new "department" or C-suite executive who has oversight responsibility for integrating and aligning legal, business and IT requirements into requisite frameworks.
6. Simplicity is the watchword and complexity is the bane of information security management. Since software, for the most part, has been written principally for functionality rather than security, this is easier said than done. However, for those organizations that put time into refining and simplifying their IT systems, the ultimate result should be more secure systems, going forward cost reductions and, ultimately, optimized IT systems.

1. These laws and regulations include the Health Insurance Portability and Accountability Act (for medical information), the Gramm Leach Bliley Act (for financial information), and Section 5 of the Federal Trade Commission Act (for consumer sensitive information).

2. These laws and regulations include the Fair Credit Reporting Act (creditors, employers and others use of consumer credit information), the Fair and Accurate Credit Transactions Act "Red Flags Rules" (financial institutions and creditors mandated identity theft prevention programs), and state security breach notification laws (required notice to consumers whose sensitive financial, medical or other information has been inappropriately accessed).

3. The Sarbanes Oxley Act, among other things, mandates internal controls, including IT controls, for financial statements.