WILMERHALE

Data Security Gains Attention from Regulators and Private Claimants

2003-05-30

The security measures of companies that collect and maintain personally-identifiable data have come under increasing scrutiny in the past few years. The U.S. federal government and certain states such as California are moving to regulate data security. This is a trend that has only begun and should prompt all companies, even if not yet explicitly required, to review their internal procedures and policies for safeguarding their data holdings.

Federal Regulations Concerning Data Security

As discussed in our May 2, 2000 Internet Alert, data security is one of the generally-accepted Fair Information Practice principles used by federal authorities to determine whether identifiable data are handled in an appropriate manner. Yet, there is no generally applicable federal data security regulation. In May 2000, a special committee of the Federal Trade Commission recommended that all commercial web sites implement security programs appropriate for the personally-identifiable data they maintain, but the FTC has opted instead to police data security practices under its traditional authority to prohibit unfair and deceptive business practices.

To date, the most significant federal regulation of data security affects the health care and financial services industries:

HIPAA Security Rule: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required that the Secretary of Health and Human Services (HHS) adopt regulations to protect individually-identifiable health information used and disclosed by health plans, health care clearinghouses that process and format health transaction data, and health care providers. The HIPAA Privacy Rule defines permissible uses and disclosures of health information and grants individuals rights to know and control how their data is used.

As discussed in our March 31, 2003 Internet Alert, the HIPAA Security Rule prescribes specific data security requirements for individually-identifiable health information maintained in electronic form. The Security Rule has a compliance deadline of April 21, 2005, or one year later for small health plans. The Security Rule requires covered entities to ensure the confidentiality, integrity and availability of all HIPAA-protected health information that the entity receives, maintains or transmits

electronically. Entities must also protect against reasonably anticipated threats or hazards to the security or integrity of the information and must protect against any reasonably anticipated unauthorized uses or disclosures of the information. The Security Rule sets out a list of eighteen standards and thirty-six implementation specifications, concerning topics such as password and login procedures, disaster recovery and contingency plans, facility security, and encryption of data. These safeguards are classified as either "required" or "addressable," with covered entities permitted to consider their size, complexity, technical infrastructure, capabilities, cost and potential risk when deciding how to implement an addressable standard. Each entity covered by the Security Rule must also implement written data security policies and procedures and maintain records of their security compliance efforts for six years.

Gramm-Leach-Bliley Safeguards Rules: In 1999, Congress passed the Gramm-Leach-Bliley Financial Services Modernization Act, mandating privacy and security standards for companies that are regulated as "financial institutions." We discussed the Gramm-Leach-Bliley privacy rule in our June 28, 2001 Internet Alert. These standards ensure security and confidentiality, protect against threats and prevent unauthorized access to nonpublic personal information about consumers. Traditional financial institutions such as banks are subject to Gramm-Leach-Bliley safeguards administered by the agencies that oversee them. Under these regulations, the Board of Directors is responsible for information security and must oversee the development, implementation and maintenance of a written security program that addresses issues including access controls, encryption, monitoring, response programs and employee training. Other entities that are "significantly engaged" in providing financial products or services to consumers, such as financial advisers, mortgage brokers, and retailers that grant credit, are subject to Gramm-Leach-Bliley safeguards administered by the FTC.

The FTC's Safeguards Rule requires covered entities to develop, implement and maintain a comprehensive information security program that is appropriate for the size and complexity of the entity, the scope of the entity's activities and the sensitivity of the information.

State Approaches to Data Security

Supplementing the industry-specific federal data security regulations, recent legislation in California will impose additional duties on companies regardless of their industry. Effective July 1, 2003, companies that do business in California and maintain computerized records must disclose any breach of security to those California residents whose personal information was or reasonably might have been acquired by an unauthorized person. By its terms, this law can be applied to companies located outside of California, as long as they conduct business in the state. When required, disclosure must be made in the most expedient time possible and without unreasonable delay. In addition, injured customers have a private right of action and can seek an injunction or civil damages, though the level of available damages is not specified.

Other states are considering laws similar to California's in the context of protecting against identity theft. Some draft bills propose that entities that know of any actual or attempted unauthorized access to personal identifying information notify each individual who is the subject of the information. The time in which the notice must be sent can vary from a set number of days to a more

vague standard of a reasonable amount of time.

Effect of European Regulations on U.S. Data Security

As discussed in our December 27, 2001 Internet Alert, the European Union has adopted a more centralized approach toward protecting personal information. The European Union's 1995 Privacy Directive contains a data security provision that requires EU member countries to require "technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access" of personal data that are "appropriate to the risks represented by the processing and the nature of the data to be protected." The EU Privacy Directive restricts transfers of personal data to the U.S. and other countries without "adequate" data protection laws. The voluntary Safe Harbor program, which enables U.S. companies to overcome this restriction, includes a data security principle under which participating organizations handling EU-origin personal information "must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction." Please see our December 6, 2002 Internet Alert for information on the Safe Harbor program.

Increasing Trend of Liability for Insufficient Security

The increased scrutiny on data security in recent years has also led to a growing number of government prosecutions and private negligence claims for data security lapses. For instance, last year the Attorney Generals of three states settled an investigation into the inadequate security measures of Ziff Davis Media Inc., which allowed the personal information of 12,000 subscribers, including some credit card numbers, to be exposed to web surfers. As part of the settlement, Ziff Davis agreed to implement a number of security measures, to pay a $100,000 fine and to pay $500 to each of the customers whose credit card information was exposed, regardless of whether the information was used.

More recently, a class action lawsuit was filed against TriWest Healthcare Alliance, claiming that its inadequate security measures allowed computer hardware containing the electronic health data of 562,000 military personnel, retirees and family members to be stolen. Even though the claim does not allege that any of the information was used for illegal purposes, the plaintiffs seek monetary damages and allege negligence, breach of contract and violations of federal privacy laws.

Self-Regulatory Initiatives

In February 2003, the Bush Administration issued the National Strategy to Secure Cyberspace as part of its Homeland Security effort to emphasize voluntary corporate action. The Strategy states that its purpose is to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact" and sets forth 47 specific actions and recommendations that are directed at individuals, government and corporations. Although the Strategy does not force companies to adopt specific security measures, it could become a benchmark for assessing future tort/negligence liability for data security breaches.

A number of organizations have also developed criteria that are more technical in nature and eventually might provide benchmarks for data security. One such entity is the Commerce

Department's National Institute of Standards and Technology (NIST), which developed security standards for use by the federal government. Other standards include the *Code of Practice for Information Security Management and the Evaluation Criteria for IT Security*, developed by the International Organization for Standardization (ISO), and the *Control Objectives for Information and Related Technology,* developed by the Information Systems Audit and Control Association (ISACA).

Steps for Addressing Data Security

In light of recent legislative and regulatory developments, companies in all industries should review and enhance their data security policies and procedures. Companies without appropriate data security measures may face regulatory action and civil liability. The new data security law in California highlights the need for companies to make data security safeguards a key part of their risk management planning and to prepare detailed policies and procedures to address both prevention of security breaches and appropriate responses, including notifications, to actual or suspected security lapses.

Authors

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089