The Changing Privacy And Security Landscape

Frederick Scholl and Jay Hollander

In a world where business practices are dominated by digital entry, storage and access to information, concerns over personal privacy and information security have escalated. Previously unheard-of issues relating to digital identity theft, alleged misuse of financial and health-related information for unauthorized purposes and even use of information to aid and abet international terrorism, have become everyday, front-page news.

This article summarizes legislative efforts to deal with some of these issues—the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act of 1999 (GLB) and the USA PATRIOT Act (2001)—and discusses security management standards that are part of the legislation. Without question, the most attention on this front has been directed to private health and financial information, as well as steps to minimize and avoid use of the digital medium to support international terrorism.

While the legislation has made protection of digital information a top priority for the financial services and health care industries, the simple truth is that all businesses need to understand and manage security better than many currently do, and most need to upgrade their security practices. Businesses that do not comply with the applicable laws risk substantial penalties mandated by these laws, as well as damage to their business reputations, lost customers and civil litigation.

Dr. Frederick Scholl is president of Monarch Information Networks, a New York-area consulting firm specializing in network forensic investigations. He can be reached at freds@monarch-info.com.

Jay Hollander, Esq., is the principal of Hollander and Company LLC, a Manhattan law firm concentrating in computer and Internet law. He is director of legal affairs for the New York City Chapter of the Association of Internet Professionals, and can be reached at jh@hollanderco.com.

HIPAA

Generally, HIPAA is aimed at administrative simplification of electronic transactional aspects of the health-care system. Although broad in scope, one of the most noteworthy portions of the law relates to developing standards to protect the privacy of individually identifiable health-care information when collected, kept and transmitted by and among "Covered Entities" within the health-care industry.

The term "Covered Entities" encompasses health-care plans and most health-care providers like hospitals and medical doctors who participate in certain electronic transactions involving protected health-care information. It also includes most health plans and health-care clearinghouses, third-party payers and insurers. Indirectly, many others, like lawyers, who acquire access to such information, will likely be affected to the extent they are defined as what the law calls "Business Associates of Covered Entities."

Covered Entities may not divulge individually identifiable health-care information without patient consent or authorization except in specific circumstances, such as for purposes of treatment, and they are to follow specific security practices to safeguard the integrity and confidentiality of protected health information, whether acquired electronically or orally, as well as to safeguard against its unauthorized use and disclosure.

Security practices include required standards and "addressable" standards; for the latter, the burden is squarely on the entity to create and then follow its own security plan. Initial requirements—primarily dealing with the management of security infrastructure and procedures—were published in the Federal Register for comments in 1998; a revised set of standards was published on February 20, 2003. Firms must comply with these standards by April 21, 2005.

As a practical matter, this means that entities must keep up with advances in security standards and try to keep up with community standards according to their circumstances. As a company goes through this audit process and makes necessary changes, prudent practice will require documenting what is being done to demonstrate good-faith efforts at compliance. When there is no precise definition of what is "enough," it helps to be able to show that you did your best in the event of a breach of security.

The other important part of the HIPPA rules concerns notice, and requires Covered Entities to provide patients with notice of the patient's privacy rights and the privacy practices of the Covered Entity. The final Privacy Rule, issued by the Department of Health and Human Services in support of the legislation, requires a Covered Entity to obtain an individual's prior written authorization to use his or her protected health information for most purposes not related to treatment or payment, with exceptions for certain public health purposes, law enforcement and other public purposes.

HIPAA's privacy rule compliance date is April 14, 2003 (April 14, 2004, for small health plans). The penalty for failing to comply is $100 per violation, not to exceed $25,000 per person per year. Criminal penalties for fraud include prison, fines and sanctions, although having an effective plan is a mitigating factor to reduce criminal penalties. There is no private right of action for patients, but failure to comply opens up possibilities for civil lawsuits, under state consumer protection or unfair and deceptive practices statutes, in addition to whatever federal disciplinary action may ensue from a patient complaint under HIPAA.

GLB

Just as HIPAA enacted privacy rules and security standards to protect against potential privacy abuses in health-care, the Graham Leach Bliley Act (GLB), which repealed previous law to allow affiliations between banks, securities firms and insurers, also took steps to protect personal consumer financial information from abuse. Its privacy protections apply to nonpublic personal information held about individual consumers and customers of financial institutions in this country; its security requirements apply to all firms holding such information.

Financial institutions are quite broadly defined for purposes of the statute and implementing rules. It includes not only banks, credit bureaus, lending institutions and securities firms, but companies like title escrow services, collection agencies, credit counselors and other financial advisers and professionals.

The legislation sets minimum standards, but rightly leaves technical implementation to each firm

GLB regulates how financial institutions may collect, use and disclose nonpublic personal financial information. It distinguishes between "customers," i.e., those with whom the financial institution offers financial products and services of any kind, and "consumers," defined as individuals to whom the financial institution offers financial products and services intended primarily for personal, family or household purposes.

It is a now a crime to submit or obtain, or otherwise cause to be disclosed, consumer information from a financial institution (including an insurer) by making a false or fictitious statement to an officer, employee or agent of the institution or to a customer, punishable by up to five years' imprisonment and $200,000 in fines.

Further, while GLB, like HIPAA, does not allow for a private right of action, GLB expressly preserves state regulatory power, in that states may enact and enforce laws that are tougher than GLB, in which case the state law would apply. Some states do have significantly stronger laws, so if in doubt about your state's regulations, consult your attorney as to which will apply in your particular state. As with HIPAA, noncompliance also may result in private and class-action lawsuits under state consumer protection laws.

USA PATRIOT Act

Unlike the restraints of HIPAA and GLB, directed at *preserving* individual privacy, the requirements of the USA PATRIOT Act are intended to require record-keeping for reporting purposes, as an aid in the fight against terrorism.

The Secretary of the Treasury was given authority under this Act to impose new record-keeping and information-reporting requirements on financial institutions to prevent money-laundering. Covered financial institutions include U.S. banks, securities brokers, investment companies, casinos, hedge funds and shell banks—businesses that deal in cash, securities or other types of assets that can readily be converted to cash. These are required to establish anti-money laundering programs under Title III of the Act. Such a program is to consist, at a minimum, of the following: a designated compliance officer, appropriate policies and procedures, training programs for employees and an independent audit to test procedures.

Penalties for failure to comply with the Act's anti-money laundering requirements, which are already in effect, are up to twice the transaction amount, with fines of $500,000 or more per transaction, for a maximum penalty of $1 million

The New Security Standards

The legislation outlined above does not specify technical standards for implementation of information security, but does set minimum national standards for the management of security information. These standards, applicable to health-care and financial institutions, are required to assure consumer privacy and to help fight terrorism.

The revised HIPAA security standards (published in February 2003 on www.hhs.gov) and GLB security standards (found in 12 CFR Parts 30, 208, 364, 570 and 748) emphasize security monitoring, testing, auditing and reporting to ensure an effective security infrastructure. Traditional risk management tools, such as firewalls, intrusion detection systems, secure protocols, etc., are *not* the focus of the security standards. Planning, design and configuration of this infrastructure is rightly left to each firm.

TABLE 1: Categories of Security Information Vendors

Function	Vendor
Visualize Information	Secure Decisions
Correlate Information	Silent Runner, Intellitactics, NetForensics, ArcSight, GuardedNet, Open Services
Data Aggregation/Analysis	Network Intelligence, Forensics Explorers
Data Collection/Analysis	FireVue, Addamark, Niksun, Eeye, Sandstorm, Wildpackets

The focus on security management is intended to ensure the quality of this infrastructure and its ability to protect sensitive information from outside and inside threats. The emphasis on monitoring and auditing recognizes that effective security cannot be achieved only through hardening of assets and erection of barriers surrounding those assets.

Meeting the new standards will require that many firms upgrade their information security in several areas. New tools for security risk management were reviewed in a recent issue of *BCR* (see January 2003, pp. 54–58). In what follows, we will provide an overview of tools and techniques for managing security information. The objective is to highlight best-of-breed features and capabilities so that the reader can then make informed product and vendor decisions.

Vendors are building partnerships in order to offer end-to-end capability

Security Information Management Tools

Security management tools collect information from networks, hosts and security devices, such as firewalls and intrusion-detection systems, and enable the user to conduct real-time and historical threat analysis and/or carry out detailed forensic investigations in the case of an actual break-in or attack. All such tools face two problems: The enormous amount of raw security data produced, and the difficulty of actually identifying real attacks in the face of the "background noise" of false positives.

Security management products therefore tend to emphasize one or more of the following functions: data collection and storage, data aggregation, data correlation and data visualization. These functions comprise collection of network traffic or logging of events, aggregation of data from the diverse security devices on the network and identification of security threats by means of correlation and/or visualization.

Some vendors attempt to provide best-of-breed solutions to one or two of the four functions. Other vendors offer products that include all the functions. As such, the marketplace is characterized by technology partnerships as all vendors seek to optimize their end-to-end capability.

Security management solutions are organized in Table 1, which indicates approximately where specific vendors fit in, at least as regards their principal focus. The table includes specialized security vendors that are complementary, directly competitive and non-overlapping. Note also the availability of broad enterprise security management offerings from IBM (Tivoli Risk Manager) and those emerging from Computer Associates.

The first group, event correlation and visualization, offers products that help identify security threats, on a real-time basis (i.e., during an attack) and/or on an historical basis for management reporting.

NetForensics has been a leader in correlation methods, including event-based rules (e.g., notify me following three unsuccessful log-in attempts followed by a successful log-in) and statistical correlation rules. Intellitactics has developed a strong correlation rule set while providing in-depth technology across all four management functions highlighted here. Open Services also provides a complete management solution while emphasizing the use of correlation to reduce false positives and false negatives.

ArcSight has added two other correlation variables including asset value (assigned by the corporate risk manager) and vulnerability status (collected from network scanners such as ISS Internet Scanner).

SilentRunner uses another approach, correlating future system traffic against past traffic. This approach does not require rules but highlights deviations from past behavior and, as such, it can detect anomalous usage patterns. SilentRunner then uses a 3-D visualization technique to display these patterns to the analyst.

SecureDecisions has focused its SecureScope product on 3-D visualization of security information. The product interfaces via JDBC with a security information RDBMS and displays three-dimensional "scenes" correlating physical security information, data security information, business function and asset information. The user must provide the security RDBMS.

The next group of products, data aggregation/analysis, is receiving increased attention as recent news events highlight the importance of data aggregation in identifying security threats. Network Intelligence has focused on expanded data-aggregation capabilities with its new LogSmart product. Each appliance, based on a hardened Win2K platform, is capable of recording 30,000 events per second sustained throughput. Multiple LogSmarts can then be deployed across the network. LogSmart is deployed with NI's enVision software, which then comprises a complete solution of data collectors and analysis software. Forensics Explorers' NetWitness is a complementary product that aggregates network packet and session information into a central data warehouse for historical analysis.

The final group, data collection/analysis includes:

- **Portable Applications:** The traditional workhorse network analyzer like Wildpackets' Etherpeek finds new life in forensic investigations. These tools are useful for "second opinion" validation of threat activity. Eeye's Iris network traffic analyzer was specifically developed for security applications and offers an easy-to-use interface, ability to search for application layer keywords and the ability to generate spoofed packets on the network.
- **Network Recorders:** Network recorders are network traffic analyzers on steroids; they allow the historical collection of packet-by-packet traffic on the network. Products such as Niksun's NetDetector, Sandstorm's NetIntercept and Forensic Explorers' NetWitness sit inside the firewall and record *all* network activity and *all* layers of packet information. This function is extremely valuable in forensic investigations. NetDetector can include up to 3 terabytes of storage with an external Fiber Channel storage device. Up to 30 days of historical information at 10 Mbps average traffic rate can be archived.
- **Log Managers:** Security appliances and host assets both produce large volumes of log file events, recording both normal transactions and possible intruder activity. Key problems in this area include massive storage problems, high event rates from multiple security appliances and the expense and maintenance of RDBMS software.

New appliances promise to make this function easier and less costly. FireVue (formerly LogLogic) has taken this approach by focusing on the Cisco PIX. The firm's Linux based LogApplicance captures up to 10,000/30,000 PIX events per second (LX1000/LX2000) using intelligent summarization to compress the log data.

Addamark's LMS uses a cluster of low-end PCs to provide high message throughput, good response time for queries and reports, high availability and low cost. Addamark does not use a RDBMS—it has developed proprietary compression and storage technology that the company claims can attain 20–40 × lower storage capacity; no DBA required. A typical five-PC cluster can handle 20,000–25,000 sustained security events per second. LMS is a component technology, requiring integration with data adapters and analytical engine modules.

Security management is a developing industry

The Future

New privacy and security information risks will require financial and health-care firms to formalize the management of security information. At the same time, technology to assist in this effort is still developing. New product features will include workflow management and configuration management during attacks. More accurate identification of real threats will be attained using concepts from artificial intelligence (AI) research.

Security management companies remain in a state of adolescence. We expect the future to include more technology and marketing partnerships, and ultimately mergers and acquisitions. As such, users should first plan their overall security information management strategy and then move carefully forward with product evaluation and implementation□

Companies Mentioned In This Article

Addamark (www.addamark.com)

ArcSight (www.arcsight.com)

Computer Associates (www.ca.com)

Eeye (www.eeye.com)

FireVue (www.firevue.com)

Forensics Explorers
(www.forensicsexplorers.com)

GuardedNet (www.guarded.net)

IBM (www.ibm.com)

Intellitactics (www.intellitactics.com)

ISS (www.iss.net)

NetForensics (www.netforensics.com)

Network Intelligence
(www.network-intelligence.com)

Niksun (www.niksun.com)

Open Services (www.open.com)

Sandstorm Enterprises (www.sandstorm.net)

SecureDecisions
(www.securedecisions.com)

SilentRunner (www.silentrunner.com)

Wildpackets (www.wildpackets.com)