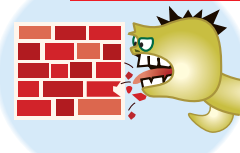


February 2003

Data Blocker



Insurers can adopt new technology tools to help them keep privacy data secure.

by Gates Ouimette

Insurers must incorporate into their operations several new international, federal and state regulations dealing with privacy and security including the Gramm-Leach-Bliley Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, the anti-money laundering USA PATRIOT Act; and state legislated opt-in/opt-out privacy mandates.

At the same time, insurers, along with the rest of corporate America's chief executives, are increasingly being held accountable for their companies' activities, and its code of ethics, as mandated by the investment community and the Sarbanes-Oxley Act.

These new rules make it difficult for insurers to determine their own increased exposure to new risks. The potential benefits are great for insurers that proactively analyze their privacy and security systems, while those that wait to react may experience negative financial, political and brand repercussions.

The new rules are particularly complex for multiline insurers doing business in more than one state. For example, they may find their obligation to comply with Gramm-Leach-Bliley complicated because it is enforced by state insurance commissioners, who use

their own state laws and regulations to track compliance with the federal rules. Fortunately, most states are following Gramm-Leach-Bliley recommendations by the National Association of Insurance Commissioners or the National Conference of Insurance Legislators, decreasing the risk that insurers could have 51 different interpretations. Regardless, as part of both the health-care and financial services industries, insurers receive potentially twice the exposure in regards to privacy compliance.

Complexity

The seemingly polar requirements of maintaining an individual's privacy with the corporate need for ready access to personal information for a multitude of business reasons were highlighted during a recent panel discussion moderated by the Massachusetts Electronic Commerce Association. Using a case study, the panel discussed a scenario in how financial-services aggregation can collide with identity theft. The case was compiled from actual incidents and known vulnerabilities that illustrated the interdependency between privacy and securi-

ty, and the points throughout the extended enterprise at which they can conflict or complement each other.

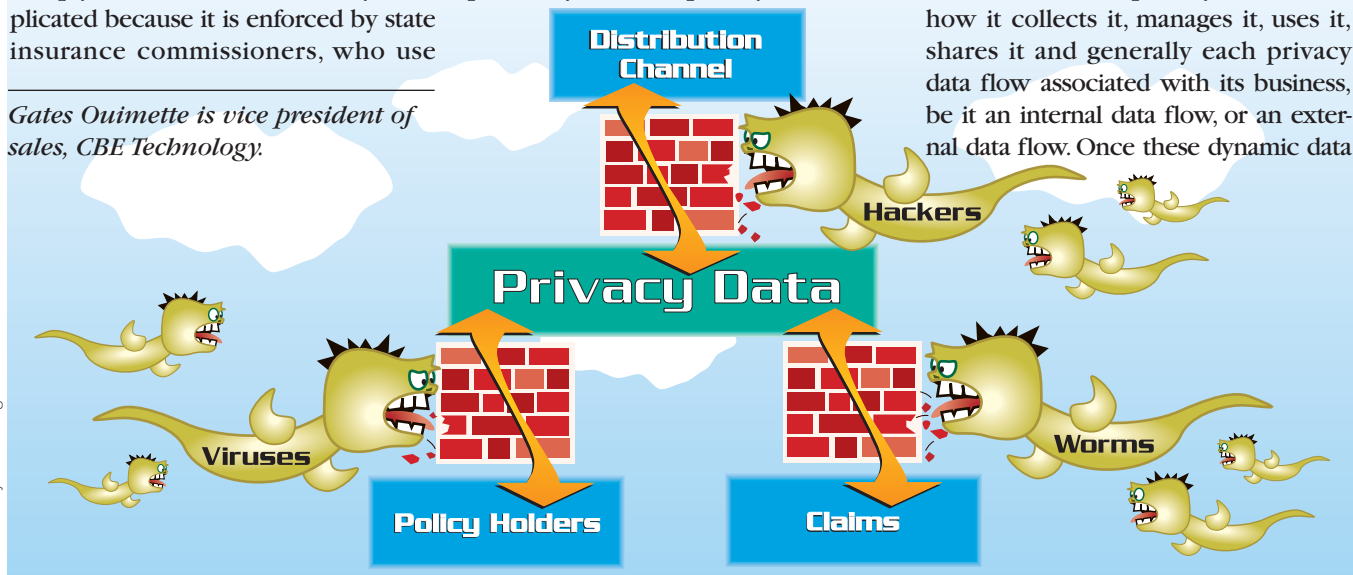
Understanding the combined privacy impact of Gramm-Leach-Bliley and HIPAA allows an insurer to begin to plan and manage the need for client/employee data privacy vs. the need to readily access that data for multiple purposes. While the complexity of privacy regulations affects the insurance industry more than other industries, insurers have always had privacy data to use, manage and safeguard so many are ahead of the curve. But with the government now more involved, insurers do themselves a disservice by underestimating the potential impact of privacy violations to their own firms.

Risk Analysis

To guard against such privacy violations, insurers should begin risk analysis with a gap analysis, a study of the differences between two different information systems or applications, often in order to determine how to get from one state to a new state. An insurer must undergo a traditional gap analysis to examine what privacy data it has, how it collects it, manages it, uses it, shares it and generally each privacy data flow associated with its business, be it an internal data flow, or an external data flow. Once these dynamic data

Gates Ouimette is vice president of sales, CBE Technology.

Illustration by Ellen Wagner



flows are captured and documented, they will need to be updated and reviewed, consistently, and constantly. Ultimately, as with any good risk analysis, an insurer's senior management must understand its risk options and, using best projections, the costs of absorbing or nullifying those risks. The important qualifier here is that privacy data risk analysis and management must become ingrained in an insurer's standard business operating procedures. The risk of not doing so, for any insurer, is becoming too great.

Technology's Role

The role of technology in helping an insurer best analyze and manage risk is evolving to encompass some of the newest technology, identity management. However, before even considering how to incorporate any new technology, the basic prerequisite for effective, efficient privacy management must be a robust security foundation.

The concept of the security fortress is no longer valid; there is a high level of certainty that an insurer will have security breaches. Privacy data is simply one type of data that must be protected during these breaches. The key, therefore, becomes how to minimize a breach, resolve the breach and manage the company's response to that breach.

As insurers deal with the regulatory reality that they must keep privacy data secure, technology becomes a tool to simplify what they have been doing for years; capturing, using and managing privacy data. By adopting the right technologies that are focused on a solid security foundation, insurers

can streamline their internal privacy processes and procedures. By doing so, insurers not only make themselves more efficient, but they increase their effectiveness in using their privacy data. Examples of technology relevant to an insurer's privacy data management function include the following:

Best practices-based security foundation: In addition to using best-of-breed point solutions such as firewalls, network-based intrusion detection, server-based intrusion detection, virus protection and data backup, insurers should analyze the merits of newer applications of technology. These include newer security policy definition/compliance tools and usage pattern matching tools from companies such as Harris. This also includes extending the security reach of existing security products such as NetScreen's firewall/virtual private networks appliances into the core of your internal computer network. This approach then enhances your overall security/privacy foundation by providing internal network encryption, an opportunity to apply differing security policies to different security zones, and secure segmentation—the ability to limit a security breach to a smaller portion of a network.

Monitoring and management tools and services: A recent Gartner Group review on the state of data security focused on the fact that most corporations, and insurers, have numerous security tools in place. However, corporations lack a disciplined process for testing, certifying, installing and monitoring/managing updates to that distributed technology, down to the

desktop/hub/router/switch/firewall/VPN level. For example, while Microsoft software is known for requiring security update patches, how many corporations leave the installed software alone once it's working? The concept of providing automatic updates to any installed Microsoft product seems to make sense, but how realistic is it to believe that allowing this without a "pre-update certification" process will not cause any application conflicts? Beyond the risk of application conflicts, there has been recent discussion that implementation of Gramm-Leach-Bliley may come into conflict with Microsoft's auto-update function. This discussion has been based on Microsoft terms and conditions requiring certain personal information to allow the update on an individual PC.

Microsoft is not unique in requiring security updates to its installed product; there have been recent security breaches in hardware products as well. Virus protection itself mandates continuous monitoring and updating.

The use of monitoring and management tools, or services, should be mandatory, in certain instances. For example, the National Credit Union Association requires firewall monitoring. As an industry based upon risk management, it only makes sense that insurers explore similar requirements for their internal systems.

Identity management: As a superset of enterprise privacy management software tools such as Zero Knowledge's Enterprise Privacy Manager and the broader category of role-based access control, identity management encompasses a multitude of approaches, tools

Identity Management

What is it? The way businesses should be administering user identity on a network using strict security standards to ensure privacy while making the information accessible to internal and external entities.

Why does it exist? So consumers feel safe using the Internet to buy items or services such as life insurance policies without worrying about intruders stealing their identity, credit card numbers or obtaining personal information.

Why is it important to insurers? The industry is dealing with compliance with several government regulations including the Gramm-Leach-Bliley Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, the anti-money laundering USA PATRIOT Act; and state legislated opt-in/opt-out privacy mandates. These regulations place insurers in the position of walking a tightrope of maintaining privacy while being asked to maintain and use personal data.

and vendors. Summarized in a June 2002 abstract of Esther Dyson's Release 1.0, identity management is "the notion of users with individual privileges and profiles." Based upon a "technical infrastructure of identity management—directories and authentication—and the primary functions they support: authorization/access/security, and credentials," the promise of identity management is when privacy data is given "electronic context." Privacy data, as a data portion of identity management, theoretically becomes both more secure—because there is no paper trail—and more functional for a user of that data.

A basic example of identity management is P3P, the Platform for Privacy Preferences Project that was developed by the World Wide Web Consortium. P3P is described on the Web site (<http://www.w3.org/P3P>) as "emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P-enabled browsers can read this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can

understand, and, most importantly, enables users to act on what they see."

Identity management is being courted aggressively by most major software vendors and numerous smaller firms such as Oblix and Netegrity. It's an area of potentially huge growth and there should be plenty of alternatives for insurers to investigate.

Business continuity planning and management tools: In its simplest relation to privacy, business continuity planning is a predefined set of best practices for managing and implementing a response to an external event. Since a privacy breach has some of the characteristics and ramifications of a potential disaster, having a tested methodology for mitigating its impact and managing a response will help any insurer respond to, and recover from, a privacy issue. A managed response, in this context, includes legal and public relations-related activities as well as technology-related activities. Tools such as the anticipated release of Mitigator v5.0 from Evergreen Data provide a self-diagnosis capability that can incorporate security/privacy risk options and costs.

While technology continues to evolve and lend itself to new applications—in this case privacy data management—the underlying requirement to the most effective use of technology for privacy protection is to have a solid, flexible, manageable security foundation. Supporting the foundation should be a proven approach to integrating existing technology "best practices" in the monitoring, management and business

continuity planning disciplines. Doing so will decrease the potential for privacy issues while at the same time minimizing their impact.

Implementation Strategy

While the privacy landscape is large, insurers could benefit from making the security and management of privacy data a priority and, in so doing, making it an integral part of the corporate culture by taking the following actions:

- Undertake some form of gap analysis of legislation dealing with privacy data.
- Monitor the legislation and audit the impact of its dynamic evolution on the information flows of your business.
- Integrate existing internal technology investments such as security, firewall/VPN appliances, customer relationship management/customer information management and monitoring/management into the objective of maintaining the privacy of privacy data. Consider integrating, in some aspect, your internal security, privacy and compliance business and technology functions with your business continuity policies, processes and procedures. These steps can potentially shift what could be purely a cost function to a possibly profitable investment.

Since privacy data is really an insurer's corporate jewels, continue to explore and consider investing in more futuristic initiatives outside of your enterprise. An example of such an initiative is MIT's Actuarinet (<http://actuarinet.mit.edu/actuarinet/brochure.pdf>). BR