The Two Sides of ROI: Return on Investment vs. Risk of Incarceration

Legislative mandates potentially replace CIO's primary concerns of technology risk management with the possibility of serving jail time.

It wasn't that long ago that IT security was viewed by CEOs and CFOs as an avoidable, low-priority expense. Many organizations charged into the new millennium with those lingering thoughts. However, Congress and the courts are forcing IT executives to reconsider, with major motivation provided by three pieces of legislation:

- The Health Insurance Portability and Accountability Act of 1996 (aka HIPAA), affecting privacy/health care industry;
- The Gramm-Leach-Bliley Act of 1999 (aka GLB), affecting privacy and security of nonpublic personal information/banking, securities, and insurance industries; and
- The Sarbanes-Oxley Act of 2002 (aka SOX), affecting accountability/business.

In this column I discuss the implications of the confidentiality, privacy, and security aspects of this legislation as it relates to IT within modern organizations, considering each piece of legislation in the order in which it was implemented.

Gramm-Leach-Bliley

GLB began life as the Financial Modernization Act of 1999. As the title implies, it deals with regulations regarding the scope and interrelationships of key financial industries: insurance, securities, and banking. (See banking.senate.gov/conf/grmleach.htm for a useful summary of all seven sections of the Act.)

Prior to GLB, these three industries were covered by stricter regulations of the Glass-Steagall Act that was enacted in response to the stock market crash of 1929. GLB sought to relieve these industries of some of the constraints imposed by Glass-Steagall. However, in deliberating GLB, Congress recognized that by enabling new types of mergers and acquisitions of financial institutions and by expanding the range of financial services these institutions could offer GLB would exacerbate consumer privacy problems. It is this latter consideration is the focus here.

GLB addresses the concern for personal privacy in Title V of the summary mentioned previously. GLB authorizes eight federal agencies and the states to enforce three rules regarding financial privacy, the safeguarding of personal information, and pretexting. The Privacy Rule requires organizations that engage in financial activity in the fairly broad sense—even down to the level of tax preparation and financial planning—provide customers copies of their privacy policy and explain their practices on sharing customer information. The Safeguards Rule requires businesses to protect the confidentiality and integrity of personal consumer information. While of

ROBERT NEUBECKER

Under GLB, due diligence now includes state-of-the-art expertise in hacking, malware, and social engineering. These are not skills over which the typical CIO has mastery.

great importance, a third GLB privacy provision on "pretexting," or the use of personal information under false pretenses, falls outside of the scope of this column.

The business part of GLB is the Privacy and Safeguards Rules. The bottom line is taken directly from Section 6801 of the legislation, the intent of which seems straightforward: organizations that engage in financial activity must respect the privacy of customer data and undertake such measures as are necessary to protect them while in their care, custody and control. If that doesn't grab the attention of IT executives, the penalties provisions meted out by the eight federal agencies certainly will. But, recalling that our focus is on IT, the real attention grabber is the implication of GLB on IT and the CIO.

To illustrate, one of the first successful GLB prosecutions was against Nationwide Mortgage and Sunbelt Lending Services for violation of the Safeguards Rule. Nationwide and Sunbelt were found remiss in their implementation of a written information security program, including the absence of a single contact for oversight of GLB compliance, the absence of a risk assessment, the absence of safeguards to control the risks, and failure to require service contracts to abide by the same security standards. In whose organizational domain do these responsibilities typically fall? The CIO. By default, GLB ports many of the more career-threatening responsibilities over to the CIO. The CIO may not be mentioned in the Act itself, but the CEO and CFO will likely ensure the CIO will play a prominent role in the accountability matrix.

An even more dramatic example is the Petco prosecution for violation of the Privacy Rule. The FTC claimed that security flaws in the company's Web site, www.PETCO.com, violated the privacy promises it made to its customers by not applying "reasonable and appropriate measures to prevent commonly known attacks by hackers…"

The privacy promise was: "At PETCO.com, protecting your information is our number-one priority, and your personal information is strictly shielded from unauthorized access. Entering your credit card number via our secure server is completely safe. The server encrypts all of your information; no one except you can access it."

The FTC interpreted this to mean that the typical customer has every right to expect that providing credit card information to Petco via its Web site is essentially risk free. Such was not the case. Petco was prosecuted because its Web site was open to SQL injection attacks. The FTC concluded it was Petco's responsibility to ensure that "reasonable and appropriate security measures" were taken to guard against well-known hacks. Again the issue of assigning responsibility arises. If your organization is prosecuted for having a Web site that is vulnerable to hack attacks, which executive do you think is going to take the fall?

The implications for the CIO and IT are onerous. Under GLB, due diligence now includes state-of-the-art expertise in hacking, malware, and social engineering. These are not skills over which the typical CIO has mastery.

GLB may be distinguished from prior legislation in many ways. Breadth and scope of purpose and the distribution of authority for administration and enforcement come immediately to mind. However, for those of us in IT, the organizational obligations

to protect consumer privacy, and the requirement to completely and accurately disclose the organization's policies, may be the most important from the point of view of long-term job security. GLB not only protects and safeguards nonpublic information held in trust, it also places the CIO, CSO, and IT management in the hot seat for covering the organization's assets. This is becoming a common theme.

HIPAA

Though HIPAA predates GLB by approximately three years, its implementation is so extensive that some of its provisions haven't yet been put in force.

Operationally, HIPAA applies to electronic protected health information (EPHI) as it relates to covered entities (CEs). EPHI covers electronic health records that contain information that can uniquely identify individuals, and CEs are the folks that routinely transmit EPHI as part of their normal operation (health care providers and insurance companies).

As with GLB, the HIPAA statute is fairly broad-based in its objectives. It has five goals:
Title I: Portability
Title II: Administrative Simplification
Title III: Tax Benefits
Title IV: Group Health Insurance
Title V: Revenue Offsets

Of these, only Title II is relevant to this column. The purpose of Administrative Simplification is to protect the privacy of the data, secure the storage and transmission of the data, and create viable transaction and code sets to exchange information between CEs. These three goals are informally referred to as The Privacy Rule, The Security Rule, and the Transactions and Code Set Rule. While I will limit subsequent discussion to the Security Rule, it should be understood that the Privacy Rule has been in effect since April 2003 and carries civil and criminal penalties up to $250,000 and 10 years in prison (see www.hhs.gov/news/facts/privacy.html); the Transactions and Code Set Standards have been in place since August 2000 (see www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/finalrule/default.asp).

Safeguard 1: Administrative

Standard 1: Security Management
- Implementation Specification 1: Risk Analysis (required)
- Implementation Specification 2: Risk Management (required)
- Implementation specification 3: Sanctions (required)
- Implementation Specification 4: Information System Activity Review (required)

Standard 2: Assigned Security Responsibility
Standard 3: Work Force Security
- Implementation Specification 1: Work Force Authorization and Supervision (addressable)

....

Safeguard 2: Physical

Standard 1: Facility Access Controls
- Implementation Specification 1: Contingency Operations (addressable)
- Implementation Specification 2: Facility Security Plan (addressable)
- Implementation Specification 3: Access Controls and Validation (addressable)
- Implementation Specification 4: Maintenance Records (addressable)

Standard 2: Workstation Use
Standard 3: Workstation Security
Standard 4: Device and Media Controls
- Implementation Specification 1: Disposal (required)
- Implementation Specification 2: Media Reuse (required)
- Implementation Specification 3: Accountability (addressable)
- Implementation Specification 4: Data Backup and Storage (addressable)

Safeguard 3: Technical

Standard 1: Access Control
- Implementation Specification 1: Unique User ID (required)
- Implementation Specification 2: Emergency Access Procedures (required)
- Implementation Specification 3: Automatic Logoff (addressable)
- Implementation Specification 4: Encryption and Decryption (addressable)

Standard 2: Audit Controls

....

Requirement 1: Organizational
Requirement 2: Policies, Procedures, and Documentation

Selected provisions of HIPAA (adapted from *HIPAA Security Implementation*).

With the exception of small CEs, the Security Rule will take effect April 21, 2005. The logic of the HIPAA Security Rule seems baroque at first glance: it consists of three safeguards and two requirements, which are further subdivided into standards and implementation specifications. Standards are required while implementation specifications may either be required or addressable. An addressable specification is one that requires attention and a documented decision to implement, not implement, or provide some alternative. The reason for the vagueness is that HIPAA's Security Rule is technology neutral. As long as an organization can legally achieve the desired subgoal, the means are essentially irrelevant.

The three safeguards with some of their attendant standards appear in the figure here. A brief example will make this easier to put into perspective. Safeguard 2 of the HIPAA Security Rule requires certain minimal standards for physical security of an

Even though the CIO may not have written the annual or quarterly report, if it is found deficient or in error because of inaccurate corporate accounting or data processing, that fact is unlikely to be overlooked by the CEO and CFO.

organization's information assets. This is spelled out in four standards that drill down from the access to the facility, through the use and security of the workstations in use, to the protection of storage devices and media.

The standard for the Device and Media Controls is to "Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility." What would that entail? Fundamentally, it involves the disposal of peripherals and media that minimizes unauthorized access. This is required by HIPAA. For a barometer of what techniques are acceptable, we look to industry standards and practices. Cross-cut shredding of removable media such as CDs and DVDs is probably acceptable, as would be melting down a hard disk into its constituent elements.

Merely erasing files with operating system file managers, however, would not be considered compliant. Software data recovery tools exist that can recover such data effortlessly. In fact, erasing data with multiple pass overwrites (for example, using the cipher with utility in Windows) might also fall below the compliance threshold because hardware data recovery tools recover magnetic residue from erased disk surfaces. However, that doesn't mean that the disks must be destroyed. HIPAA is accommodating of exceptions like hard disk reuse/repurposing, as long as the spirit of the law is followed. In such a case, documented chain-of-custody with a multipass disk erasing tool that complies with some government standard, such as DOD 5220 22-M, would likely be considered acceptable. We could then document that our disk cleaning policy complies with the latest DOD standard for the prevention of both hardware and software recovery of data. Again, HIPAA does not specify how we dispose of devices and media, but just that we do so in such a way that the information therein is protected from unauthorized view. One would approach other standards and implementation specifications similarly.

A quick review of the fragment of HIPAA Safeguards listed in the figure here will reveal that there are many implementation problems in the compliance world, most of which fall within the purview of the CIO. What happens if the data on one of our elusive, data rich, partially wiped disk drives gets posted on the Internet (this has happened). Or suppose some spyware accompanies a gratuitous Web access and shares confidential data. Or imagine a user walks away from an unprotected, unlocked workstation and a bystander gains access to a health record. These breaches all fall within the CIO's IT domain. As with GLB, they also carry a stiff penalty. Civil penalties for HIPAA violations range from $100 to $25,000, and criminal penalties escalate to a $250,000 fine and/or 10 years in prison.

The implications for the CIO and IT are worrisome. Under HIPAA, due diligence now includes state-of-the-art expertise in hacking, malware, and social engineering. These are not skills over which the typical CIO/CSO has mastery.

Sarbanes-Oxley

SOX was the Congressional response to the corporate and accounting scandals that span the 15-year interval between the Salomon Brothers bond-trading scandal and the Enron and MCI-Worldcom incidents. Congress is making a definite statement with SOX: the "sleight-of-hand earnings" accounting philosophy that crept into U.S. business, and the excuse "I just can't recall" just won't cut it anymore.

While no one would accuse

Congress of being quick to act, by all admissions it did act decisively with SOX. The Preamble to H.R. 3763 makes it clear that SOX seeks "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws." SOX attempts to achieve this goal by setting higher standards for corporate governance and accountability, financial disclosure, and the practice of public accounting.

SOX is actually addressed to the CEO and CFO. Under Section 302, both must certify in each annual or quarterly report that: they reviewed the report; the report does not contain any untrue statements or omissions of a material fact; the financial statements are accurate; they assume responsibility for the report and internal controls; they have disclosed all material facts and deficiencies to the auditors, and any fraud, whether or not material, that involves management or employees who have a significant role in the internal controls; and they have listed any relevant changes in internal controls or other factors that would reveal deficiencies or material weaknesses.

That doesn't leave much flexibility. The CEO and CFO must both tell the truth in the reports, inform on their greedy colleagues who have engaged in fraudulent behavior, and then take responsibility for everything. The list of penalties in Title IX of SOX is going to make the corporate top-down looters squirm a bit. For example, Section 1350 provides a penalty of up to $1,000,000 and 10 years imprisonment for basic non-compliance, and $5,000,000 and 20 years for willful non-compliance. This is not to mention the "Fair Funds Provision," by which the courts may elect to hold executives who make false disclosures personally liable to their investors.

But forget all that, we want to see where the CIO fits in. We don't have to look far. The CIO is drawn into SOX at virtually every turn.

Let's start with Section 302. How would management and employees most likely perpetrate the fraud? It's probably not by pawning the office furniture. Nor is it likely to be hauling out pickup loads of cash from the vault. In all likelihood, an insider fraud would involve some compromise of a computer or network system that is under the control of the CIO.

Additionally, Section 404 of SOX requires that the internal control reports must "state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and contain an assessment … of [its] effectiveness." Well who is in charge of the data on which these reports were based? The CIO. So Section 404 of SOX brings the CIO to the certification table. Even though the CIO may not have written the annual or quarterly report, if it is found deficient or in error because of inaccurate corporate accounting or data processing, that fact is unlikely to be overlooked by the CEO and CFO.

What is more, Section 409 of SOX holds that organizations are expected to disclose material information to the public "on a rapid and current basis such additional information … as is necessary or useful in the protection of investors and the public interest." Let's consider this for a moment. What division of the organization has the capability of reporting disclosures like this in real time? Again, this has the CIO and IT written all over it.

Because electronic data processing is a staple of modern business and industry, provisions of SOX impose considerable responsibilities on the modern CIO. SOX makes it the CIO's responsibility to put fraud detection systems in place, prevent inside compromises of the IT environment, block unauthorized access to trade secrets and confidential information, secure the information infrastructure from external attack, determine the effectiveness of IT control mechanisms, perform routine IT security audits, and prevent other IT activity that might compromise investor equity. By any measure this is an enormous responsibility.

Conclusion

I've drawn attention to HIPAA, GLB, and SOX to show how the burden of risk management has slowly but surely moved toward the CIO. Even in the case of SOX, where the required certifications are

signed by the CEO and CFO, a great deal of the responsibility for accurate reporting falls on the CIO. The challenge for the modern organization will be to find CIOs who are prepared for the challenge.

These three laws will change the role of the CIO forever, I predict. While 10 years ago their biggest fear was obsolescence and technology inversion, now they face jail time. In the current climate the CIO position is not a good career goal for ulcer-prone individuals. But, by the same token, this is a real opportunity for top-quality upper managers with superior IT security skills to move into an executive suite.

HIPAA, GLB, and SOX are not set in stone. As I write this, there are detractors who feel the legislation is draconian and prohibitively invasive. Legislative mandates mirror the swing of the pendulum, and it is possible, if not likely, that some provisions of this and future legislation will soften the treatment of executives who have steered their corporate ship aground. That said, the one part of HIPAA, GLB, and SOX that is likely to remain in nearly full force is corporate and organizational accountability. And in the new millennium, accountability amounts to record keeping, fraud prevention and reporting, data security, as well as risk management and mitigation in the IT department.

My advice to all CIOs is to ensure your skills are appropriate for the challenge, that your IT house is in order, and then request an increase in your compensation package for all of the new risks that have come your way. C

Hal Berghel (www.acm.org/hlb) is a professor and the director of the UNLV School of Computer Science, and director of the University's Center for Cybermedia Research and co-Director of the National Identity Theft and Financial Fraud Research and Operations Center.

URL Pearls

The primary U.S. Government resource for detailed information regarding legislation is Thomas (thomas.loc.gov). Anticipate information overload if you use Google: there are approximately 4.5 million hits for "HIPAA," 216,000 for "Gramm-Leach-Bliley," and 1.86 million for "Sarbanes-Oxley."

Other resources include: background information on Gramm-Leach-Bliley is available from the Senate's Banking, Housing and Urban Affairs Committee Web site at banking.senate.gov/conf/. Also see the GLB link on the Federal Trade Commission's Privacy Web site at www.ftc.gov/privacy/ that includes links to other important privacy legislation. See www.ftc.gov/os/2003/031223anprfinalglbnotices.pdf for a list of the federal agencies involved, and the interagency form used for compliance. An independent overview of Gramm-Leach-Bliley is available at the Electronic Privacy Information Center: www.epic.org/privacy/glba/.

Details concerning the Nationwide/Sunbelt and Petco prosecutions are available at the FTC GLB site: www.ftc.gov/privacy/glbact/.

Health and Human Services has its own HIPAA Web site at www.hhs.gov/ocr/hipaa, complete with regulation and statute summaries, compliance information, access to online information, and related links to the Privacy Rule, the Security Rule, and Transactions and Code Set Standards in a variety of downloadable formats. A copy of the actual document of Public Law 104-191 is available at aspe.hhs.gov/admnsimp/pl104191.htm. The best overview of HIPAA that I know of is *HIPAA Security Implementation*, published by SANS Press, August 2004 (a revision is likely soon); this is a must-have if you're involved in IT in a covered entity.

Sarbanes-Oxley has its own Web site at www.sarbanes-oxley.com. A PDF copy of H.R. 3763, along with useful summaries and commentary, are available at the Financial Executives Web site: www.fei.org/advocacy/sarbanesoxley.cfm.

Pretexting is a huge societal problem, most especially because it may lead to identity theft. GLB makes it illegal to use any of the following instruments to obtain customer information:

1. False, fictitious, or fraudulent statements,

2. Forged, counterfeit, lost, or stolen documents,

3. Ask anyone else to do 1. or 2.

While GLB and the Federal Identity Theft and Assumption Deterrence Act make such activities federal crimes, they have yet to effectively derail identity theft—now the leading white-collar crime. C