

Identity Theft's Impact on the Information Security Program

By Pamela Fredericks

Identity theft is usually considered to be a consumer issue rather than a corporate one – a matter of privacy rather than security. However, it is both of course, because there are now two types of data in most organizations.

Identity theft is usually considered to be a consumer issue rather than a corporate one – a matter of privacy rather than security. However, it is both of course, because there are now two types of data in most organizations. Companies harbor both their own proprietary data and significant amounts of personally identifiable information belonging to customers, clients, and business partners. There are security measures that must be taken for all information, and special privacy and confidentiality requirements for data belonging to others.

At this early stage in the coexistence of these two classes of data, the information security program behaves something like a busy intersection that has yield signs rather than stoplights. Frequent “accidents” occur, with breaches of sensitive information reported with frightening regularity. So, predictably, the cops are cracking down; consumers are seeing public warnings and more legislation targeting prevention and disclosure of these types of breaches.

Unlike most other countries, the U.S. has no overarching privacy or security law covering all types of sensitive information, and enforcement of privacy lapses is infrequent at best. It's often up to those charged with information security to figure out the best way to keep the identity thieves out. Because the “information” in information security has taken on a broader definition, the security program must adapt.

Identity theft incidents

The number of identity theft incidents reported to the Federal Trade Commission (FTC) continues to rise, with nearly 256,000 complaints registered in 2005 – a 37 percent increase over the previous year. The FTC reports that fraud cases targeting credit card (26%), phone or utilities (18%) and banking (17%) information were most commonly involved¹.

The enormity of the problem is perhaps best demonstrated by the chronology of reported incidents² since ChoicePoint was required by the California SB-1386 / 1798.29-82 “Notice of Security Breach” law to make a disclosure in February 2005. Between then and August

2006, at least 250 incidents have been reported resulting in unauthorized release or loss of information affecting 90,925,922 records. The summer of 2006 has been alarming, with a sharp increase in reported incidents compared to previous months. Where the average incidents per month had been about 13, in June and July there were 42 and 32 incidents reported respectively, a rate of more than one security breach per day. It is likely that more incidents occurred but are not on this list or were not disclosed.

From a security perspective, these incidents seem to fall into three main categories: theft (usually of laptops), hacking, and what is often somewhat kindly referred to as “inadvertent disclosure.” Ironically, it is quite easy to draw a parallel between these categories and the three most commonly cited safeguards of security in the legislative specifications found in the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) regulations. Laptop theft is a *physical* security issue; hacking prevention falls under *technical* safeguards; and various breakdowns in process can be prevented with *administrative* security controls. Finger pointing is easy: The root of the problem can be squarely traced directly back to failures of classic “Security 101” controls found in the information protection program.

The foundering of these basic security controls might be prevented, in part, if security compliance were not so complex. In recent years, IT departments have been buried trying to support multiple, discrete regulatory programs. While there are overlapping standards, control objectives, and frameworks, there has been little unification or harmonizing of their commonalities. Though its profile has been raised, and it is no longer underfunded, as we shall see, security remains a generally understaffed function, especially when the extra burdens of compliance are added to the mix. But compliance and security program enhancement come in several guises, including actual laws, industry standards, audit frameworks, and international standards.

Legislative response

Congress has not yet agreed on the best ways to legislate privacy and security. Competing considerations of protection versus flexibility are found in nearly every attempt to define and scope the problem.

1 <http://www.ftc.gov/opa/2006/01/topten.htm>

2 <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Security mandates must be both broad and flexible, and they must meet the needs of the particular organization or industry.

All US organizations are bound by Section 5 of the Federal Trade Commission Act (FTC Act), which prohibits “unfair or deceptive acts or practices in or affecting commerce.” Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information. This law also requires companies holding sensitive data to have in place procedures to secure it if the failure to do so is likely to cause substantial consumer injury.

Federal laws to date have targeted government and specific industries such as healthcare and financial services, but have stopped short of covering all sectors and industries. The banking industry is perhaps hardest hit. Multiple agencies (OCC, FDIC, OTS, and others) issued an interpretation of the Gramm-Leach-Bliley Act (GLBA) called the Interagency Guidelines, which clarifies financial institutions' responsibilities under that law. Separate guidance has been issued by the FFIEC for Internet banking, by the SEC for record-keeping requirements, and by international forums such as those outlined in the Basel Accord. Financial markets also face compliance with Critical Infrastructure Protection (CIP) and PATRIOT Act mandates that protect the national infrastructure through general security and anti-money laundering (AML) requirements.

Following in the footsteps of the landmark California SB-1386 Notice of Security Breach law, there are now more than 34 states filling in some of the gaps with their own notification laws and protection of other sensitive information, like social security numbers. Some federal laws, such as the FACTA Disposal Rule, contain common-sense protections for sensitive information that, if they had been in place for all types of data, might have prevented some of the recently reported thefts. (Recycled paper containing credit card data and information on stolen laptops come to mind.) The FACTA Disposal Rule requires businesses to take reasonable and appropriate measures to prevent unauthorized access to – or use of – information in a consumer credit report. Measures include destroying paper documents, erasing electronic files or media, and due diligence on third-party disposal companies.

In this most recent debate, a key reason for the delay is determining the notification “trigger” for disclosing breaches. Everyone agrees that consumers need to know when their privacy may have been compromised, but when and how often to notify is a point of contention. Privacy advocates want language similar to the original California law, which requires disclosure of security lapses regardless of potential for harm. But companies are concerned with the administrative and financial impact of notification, and prefer to use more flexible language that would limit notification to only those breaches that could cause a “significant” risk. Whatever the decision, it is likely that a single federal law will trump stronger state laws on the books.

The date is getting closer. Traditionally, strong enforcement actions from government bodies signal a legislative event, and the \$10 million-plus penalty lodged against ChoicePoint is a sign. FTC Commissioner Pamela Jones Harbour stated on March 10th that she would like to see legislation that provides stiff civil penalties in the case of a data breach that results from poor security practices³. Security has always been largely a business-driven, self-regulated and self-enforced function, but it is very about to be legislated across the board.

3 <http://www.ftc.gov/speeches/harbour.htm>

The “laws” of industry

Government is not the only source of compliance requirements. Industry has also responded to the need for identity theft prevention. The Payment Card Industry Data Security Standards (PCI DSS)⁴, issued in 2004, make one visible attempt to protect a major target. The Standards apply to any business that stores, process, or transmits credit card information. Originally instituted in 2001 as the Cardholder Information Security Program (CISP) by VISA, it is a must-do for affected businesses. PCI DSS's set of 12 basic security requirements and more detailed sub-requirements range from strong controls around data storage and encryption to basics like security policy, monitoring, and recovery.

Many businesses assumed these were already present in their security program, but are finding with a shock that they are not. Deficiencies are generally found in a lack of a data classification and documentation. VISA, MasterCard, American Express, Discover and their related banks are ready to send their auditors to ask those questions, and can lodge significant penalties or remove privileges where companies come up short.

The trend toward outsourcing and the frequency of “lost tape” incidents helped inspire the institution of another industry measure called the Financial Institution Shared Assessments Program. This program was announced in February 2006 by six major banks, and is still in its early stages⁵. It aims to create standardized IT outsourcer risk management assessments to aid banks in shopping for vendors. The move creates market pressure on computer service providers to be more systematic about disclosing their own efforts to protect sensitive data.

These are only two examples among many industry standards which, although they are not laws, behave like laws in terms of requirements and enforcement of penalties. Multiple and often overlapping standards exist in financial services, healthcare, agriculture, energy, manufacturing, retail, telecommunications, transportation, and other industries, each with its own set of standards and guidelines to address information protection.

Auditors have an impact too

Even aside from Sarbanes-Oxley, COBIT and COSO, the audit community has weighed in on personal information protection with the Generally Accepted Privacy Principles (GAPP). The American Institute of Certified Public Accountants (AICPA) and its counterpart, the Canadian Institute of Chartered Accountants (CICA), jointly established a privacy task force. The framework they created forms the audit criteria for tests of privacy effectiveness in North America. The GAPP contains 10 privacy components and 65 criteria essential for evaluating proper protection and management. Available from the AICPA and CICA Websites, it also contains a comparison to international privacy concepts, an important bridge for multinational and globally connected businesses. Any organization wishing to understand how to protect employee or customer data in any format, or seeking guidance on data retention and data destruction, may want to become familiar with this work.

4 http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf

5 Bank of America, Bank of New York, Citigroup, J.P. Morgan Chase, U.S. Bankcorp, Wells Fargo.

International perspective

These recent laws and privacy frameworks indicate that the US is finally truing up to data protection standards that have long been enforced in other countries. The 1998 European Union "Directive on Protection of Personal Data" mandated that EU member countries enact their own privacy laws, based on standard principles. The individual laws continue to be updated with nuances and improvements to the original provisions as they become more mature. In the Asia Pacific region, approaches such as the APEC (Asia-Pacific Economic Cooperation) Privacy Framework⁶ have been established. Similar to the Fair Information Practice Principles that underlie many protection laws, the work of the APEC forum seeks to enable cross-border data flows through its nine privacy principles.

Security spending reflects trend

Identity theft fears are getting everyone's attention. A study conducted by the University of Texas' School of Management concluded that publicly traded companies suffer severe and immediate financial consequences as a result of Internet security breaches. According to the study, companies lose 2.1 percent of their market value within two days of a breach becoming public knowledge. This is translated to an average of \$1.65 billion in lost market capitalization⁷.

IT budgets reflect the trend. Sarbanes-Oxley and other regulations have had a huge impact on IT controls and spending, as shown in a Spring 2006 McKinsey & Company report⁸. According to the CIOs surveyed, 46 percent of the 2006 IT budget – nearly half! – is earmarked for security, regulatory support, and reliability initiatives such as business continuity and disaster recovery. Security spending also occupies both the first and second priorities for technology spending over the next 12 months, according to recent Morgan Stanley research⁹. Security professionals have long waited for this kind of focus and commitment from management.

Unifying compliance requirements

Protections against identity theft reside in the information security program, and today that program is necessarily grounded in compliance. The only way to make the overwhelming complexity of laws and standards practical is to simplify it. Organizations should build a matrix that aggregates and aligns those requirements applicable to them. These security requirements will originate from the business, from applicable federal and state regulations, and from pertinent industry standards or frameworks.

This coordination of the compliance effort is important to its success.

Once the requirements are captured, the more difficult task is finding the commonalities among them. Creating this matrix will almost certainly require a breadth of knowledge no single person is likely to possess. An understanding of information security controls,

privacy concepts, business objectives, legal foundations, and audit will be needed.

Fortunately, because security's profile has been raised to one of operational risk, there may be a pre-existing committee of security stakeholders who can provide the needed perspectives. If not, such a forum may need to be created. This coordination of the compliance effort is important to its success. For public companies and others who have implemented internal controls programs to satisfy Sarbanes-Oxley 404, such a matrix and a coordination committee may already be in place.

The standards bodies and the audit community have numerous frameworks and methodologies designed to organize and harmonize security controls. COBIT, nearly synonymous with Sarbanes-Oxley, helps define and manage IT processes and identify appropriate controls objectives. ITIL, a back-to-basics set of service-oriented processes, has taken a somewhat surprising foothold in many organizations. ISO/IEC 17799, *Information technology -- Security techniques -- Code of practice for information security management*, was updated in 2005 and remains the primary set of security best practice basics, organizing security in a way that is intuitive, accessible, and audit ready. A counterpart but lesser known international standard, ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*, provides the control objectives and control statements for each of ISO 17799's best practices.

Back to the classics

Definitions of security vary, but all security programs essentially have the same goals and the pretty much the same ways of getting there. Security can be defined generally as "the set of measures by which organizations protect information from unauthorized access, disclosure, alteration and destruction." Another common definition cites the principles of confidentiality, integrity, availability, and accountability. Or, at its very simplest, security is a set of controls for physical, administrative, and technical security. However it is broken down, there will be a finite number of categories into which all security requirements can be aligned. There is no magic to it: auditors and regulators are not looking for anything else.

One good set of basic security control requirements for corporate data is:

| | |
|------------------------|--|
| Availability | Physical security and systems maintenance ensure the business can be served. |
| Recoverability | Business continuity and disaster recovery plans provide stability. |
| Confidentiality | Privacy for sensitive information. |
| Data integrity | Security for access control and accuracy. |
| Accountability | Audit and monitoring controls provide metrics. |

It is important to remember that information security is an ongoing process, a continuous life cycle. Security policies and technical controls must be based on identified risks to assets. Controls should be reasonable and appropriate in light of the circumstances. And a breach does not necessarily show that a company failed to have rea-

6 <http://www.apec.org>

7 http://som.utdallas.edu/faculty/papers/faculty_pubs.php?pbt=4

8 http://www.mckinseyquarterly.com/article_page.aspx?ar=1745&L2=13&L3=13

9 Morgan Stanley Equity Research, January 3, 2006, "Enterprise Technology: Morgan Stanley CIO Survey"

sonable security measures, because there is no such thing as perfect security. Auditors realize that humans work for organizations, and sometimes even the best set of controls will falter. Regular audits, continuous monitoring, and periodic reassessment of risk are the essential elements of an information security management system.

Making it happen

The best approach for companies to keep themselves off the front pages of The Wall Street Journal (and to avoid sending out those letters to customers that begin, "Your privacy is very important to us, but...") may in fact be the most obvious and simple one. It requires two things: a unified compliance framework and a relentless focus on classic information security controls. Combined with an eye to-

ward auditability, this approach will not only prevent most identity theft losses in the first place, but will also provide the most solid defense against overload in the face of coming legislation.

About the Author

Pamela Fredericks, CISSP, CISM, CIPP, has extensive experience in internal corporate information security management and administration, as well as external consulting. As senior technical consultant at Forsythe, Fredericks focuses on security controls and information privacy, with particular emphasis on security management through creation of IT policies and guidelines that fulfill security, audit, and legal compliance requirements.