

Title: Security in the Age of Privacy**Date: 8th September 2001**

Does the current debate over privacy really make a difference to information security practices? What new technologies are emerging to address this area, and how should companies be positioning their security strategy to maximize their ROI.

The job of protecting an organization's information assets has never been easy, but if you are tasked with this job, you already know that. You also know that the crux of the job is a balancing act. You must balance the risks of loss against the costs of risk mitigation. This was tough enough to do when most organizations were focused on keeping their systems, and their data, to themselves. Then came a tidal wave of change, powered by the combined forces of the Internet, distributed computing, outsourcing, strategic alliances, business process reengineering, customer relationship management, and e-business. The focus switched to sharing, not just information, but systems as well. And now, even as the effects of these enormous changes continue to wash over IT departments everywhere, a new factor is building: privacy.

Privacy has been building as a factor in the information security equation for some time (see Stephen Cobb's column in the March 2000 issue of Business Security Advisor). But there has been a tendency to bracket privacy as just another aspect of security, rather than a separate issue in its own right. Privacy and security are in fact quite different (as was pointed out in the first of these articles, published in the online edition of the August issue of Business Advisor).

Privacy refers to a value. To differing degrees, in different cultures, it is a right as well as a value. But in the context of corporate information security, the term security does not refer to a value, but rather a methodology and a technology. As such, security is neutral; it can serve privacy or hinder it. For example, a company may feel the need to filter outgoing e-mail to prevent company secrets being sent to places they shouldn't go, but that implies the reading of employee e-mail, which some people consider to be an invasion of privacy.

While information system security is typically defined as protecting the confidentiality, integrity and availability of data and the systems which process it, this definition contains a number of assumptions which transform "security" from a human value into an technical objective. For example, ownership of data and the right of the owner to restrict access to that data is implied, yet ownership of data is a central issue in the electronic privacy debate. In the U.S., much of that debate is being driven by people who think the current legal protections for electronic privacy are inadequate. Referring to themselves as privacy advocates, they are the force behind organizations such as EPIC, the Electronic Privacy Information Center.

Privacy Principles and Security Challenges

EPIC defines privacy protection as the right of individuals to control the collection, use, and dissemination of their personal information that is held by others. As you may recall from the previous article in this series (Business Advisor, October 2001) this definition is central to the Data Privacy Principles developed by the Organization for Economic Cooperation and Development (OECD); an early effort to harmonize different national data protection and privacy legislation schemes, to ensure the free flow of economically necessary personal information. While these principles were put

forth long before the commercialization of the Internet, they helped to shape the fair information practice principles to which the Federal Trade Commission frequently refers. They are:

- (1) Notice/Awareness;
- (2) Choice/Consent;
- (3) Access/Participation;
- (4) Integrity/Security; and
- (5) Enforcement/Redress.

While the fourth principle directly refers to security and integrity, and is fairly obvious in its implication, the first three principles can be seen as more subtle security challenges, of increasing magnitude. Let's take them in order.

Notice is something that should be familiar to security professionals. Many systems, including many web sites, put users on notice with respect to security. It might be a banner that appears during network logon, warning that access to the network is restricted to authorized users. It might be a splash page at the entrance to a web site, which informs visitors that clicking to enter constitutes agreement to the terms of use. It could even be a link from the home page of a site labeled Terms of Use. All of these are tools that security managers can use to make their job easier. Not that such notices prevent unauthorized access, but they certainly deter a certain amount of it, and make it much easier to prosecute and convict offenders.

Notice in the privacy context means advising users of what your policies are with respect to any personal data you collect. In itself, this is not a security issue. But to the extent that security people like to keep a company's overall risk profile low, they will want to make sure that privacy policies are properly posted, reducing the chances that the system will be targeted by privacy "hacktivists," or draw undue attention through adverse publicity.

In the same vein, choice and consent should be addressed with sensitivity. Privacy advocates prefer the opt-in form of consent, in which people specifically agree to a certain use of their information, versus opt-out, which implies the data will be used unless the owner of the data requests that it not be used. Marketing departments may need to be discouraged from pseudo-opt-in, which pre-selects Yes in the "Use my data" check box on a form. This has proven to be particularly annoying to the privacy-sensitive.

Access and participation are the real challenges as far as security is concerned. They refer to people's ability to access data about themselves, in other words to view the data about them which you have in your files, and to contest that data's accuracy and completeness. Both privacy advocates and the FTC have said that to be meaningful, access must encompass "timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients." Many systems currently lack the means to implement such processes securely, but having to do so may become mandatory at some point.

Tools to Help

Security professionals are accustomed to using tools to help get the job done, such as network scanners to find vulnerabilities on a network. Products are already emerging to help implement and audit privacy policies. For example, the company PrivacyRight provides privacy middleware, to provide a single, secure touch-point for a consumer's collected information within an enterprise's existing customer-information management structures. Their TrustFilter suite uses a Permissions Engine, a Java-based enterprise middleware platform that enforces privacy regulations, policies, and preferences, "by evaluating requests for data and comparing them to dynamic access-control rule sets."

Another player is IDcide, whose PrivacyWall family of software products enables companies to ensure their Web sites do not violate privacy. They claim that PrivacyWall thoroughly analyzes even the most complex Web sites and reports about everything that is crucial for the person in charge of privacy to know. For example, a PrivacyWall system should be able to highlight all the personal questions asked anywhere on the site, warn about Web constructs that cause leakage of sensitive personal information, and discover Web pages that accidentally publicize personal information.

One possible tool that is not so much a product as a technology is P3P, The Platform for Privacy Preferences, being developed by the W3C, and described as "a simple, automated way for users to gain more control over the use of personal information on Web sites they visit." As this technology gets closer to implementation, in the next generation of web browsers from Netscape and Microsoft for example, some critics are saying it is far from simple. However, the goal is for P3P to be, at its most basic level:

"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."

When someone visits a P3P-enabled web site using a P3P-enabled browser, the browser compares the site's privacy snapshot to the consumer's own set of privacy preferences. In this manner: "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." Given that this description is the one provided by W3C it is interesting to note the apparent dichotomy between the implied automagical comparison of site to user privacy preferences, and the emphasis on users doing it for themselves.

Indeed, this has led to criticism from privacy advocates who claim that P3P will not work because users will not want to read all of the different privacy policies they encounter; thus they will turn on automatic negotiation, with very broad settings so as not to slow down their surfing, much like users currently do with cookie settings and security settings. This particularly irks some privacy advocates because P3P sidesteps the question of what online privacy standards should be, and facilitates the coexistence of a wide range of approaches to handling personal data, some of which may be very invasive. Add to this the lack of any enforcement capability in P3P, which means a site can claim to follow certain standards in principle while violating them in practice, and you have the makings of a long and heated debate. Thus it remains to be seen whether or not P3P will become a useful tool for managing the notice, consent, and access aspects of privacy management.

Conclusions

Privacy has four main implications for information security management. First of all, rising concerns over privacy will increase the potential damage to your company from a security breach that exposes personal data. In other words, the time to tighten up security is now, rather than later. Second, you may need to bring security measures into line with standards established by legislation and rule-making, such as HIPAA and Gramm-Leach-Bliley (see Resources for what these are). Third, you may be called upon to provide technical advice and feasibility assessments to the people charged with privacy policy creation and enforcement (in fact, despite the extra work it may entail, you might want to seek out this role so that things don't get too unrealistic too soon). Fourth, in any security design work or product selection you do, there should be a strong emphasis on highly granular access controls. The chances are that you will be getting more and more requests to facilitate tightly controlled access to very specific, and very sensitive, personal data.

- Mike Cobb, MCDBA, CISSP

Resources

The first article in this series:

<http://www.advisor.com/Articles.nsf/aid/COBBM73>

The second article in this series:

Business Security Advisor, October 2001.

HIPAA security standards for medical data

<http://aspe.hhs.gov/admsimp/bannerps.htm#security>

GLB security standards for financial data

<http://www.ots.treas.gov/docs/73112.pdf>

Privacy Online: A Report to Congress

<http://www.ftc.gov/reports/privacy3/toc.htm>

Trust-e, Privacy Seal service

<http://www.truste.org>

Better Business Bureau, Online Privacy Seal Program

<http://www.bbbonline.org/>

WebTrust, privacy-certification program

<http://www.cpawebtrust.org/>

IDcide, corporate privacy compliance software

<http://www.idcide.com/>

PrivacyRight, privacy and permissions management

<http://www.privacyright.com/>

ePrivacyGroup, privacy services

<http://www.eprivacygroup.com>

IBM, privacy services

<http://www-1.ibm.com/services/security/privacy.html>

Ernst & Young, Privacy Assurance and Advisory Services

<http://www.ey.com>