

# The Corporate Culture Perspective

By Pamela Fredericks, Forsythe

Organizations are in the midst of a cultural evolution, one that is making information security and privacy protection part of expected corporate behaviors. For employees, data breaches and the reality of identity theft have driven home the importance of privacy and protection for personal data on the job—the data in the corporation might well be your own.

For IT, security no longer occupies the “nice to have” category at the bottom of the IT agenda, but has gone straight to the top of the list. If there is no security budget, something must be wrong. The overall result is a corporate shift in attitude, a new mindset where security and privacy controls are increasingly internalized and are slowly becoming standard business practices. At least four elements have contributed to this cultural change.

## Operational Risk

Security has become part of operational risk. First, information security practices are becoming part of the corporate culture because the majority of organizations now have in place at least some formalized security controls. Whether motivated by regulatory and audit requirements or by partner and customer demands, companies have realized that security controls and attention to privacy are simply good for business. Best practices, laws and standards have routinely cited the importance of a security program that is continuous and ongoing.

Still, until the last several years, security in many companies was often viewed as an obligation rather than a willingly provided service. By now, however, justification and ROI for information protection measures are often no longer required—simply say the words “security controls required to manage corporate risk” and a business case can often be made for new technology, headcount or processes to support security.

## Privacy is Personal

Second, the information a company maintains has become broader and increasingly personally identifiable. This hits home with employees and others who use corporate computer systems. Personal information can be tracked

through the sales department, human resources, accounting, IT, via Web sites and even through outside service providers. Social Security numbers, credit card or financial information, and other personal data can potentially be stolen at any entry or storage point. To employees, the need for strong passwords and other measures to control access no longer seems like an annoyance, but an expectation. Now when the security team explains to employees why it’s against company policy to share passwords or post them near workstations, they listen and might even ask where the protections are if they are absent.

## Breach Notification

According to the Privacy Rights Clearing-house, there have been over 500 security breaches since 2005, many involving the most respected organizations in the United States. California’s landmark SB-1386 laid the groundwork for more than 35 other states to enact similar breach notification laws.

Specifics vary from state to state, but each law defines what constitutes personal information; who must be notified and when; and any exceptions such as encryption or a “harm threshold.” A harm threshold is a notification that must be made only if there is a reasonable possibility of identity theft. Breach prevention now also requires that information be readily identified as triggering one of the laws. Equally important, an incident response plan must be created to fulfill the legal requirement and handle consumer inquiries and remediation. All of this has led companies to seriously take stock of personal information in their systems, scale back on what is kept and tightly secure what is retained.

Retention is also a key point for “e-discovery” since a change to the Federal Rules of Civil Procedure late last year made all electronic information discoverable—a topic with many new implications for organizations and how they classify and store data.

## Privacy as a Profession

Nearly every Fortune 100 Company now has a chief privacy officer; there is also an expanding base of credentialed individuals who hold the Certified Information Privacy

Professional (CIPP) certification from the International Association of Privacy Professionals.

**cul-tured** *adj.* having refined taste and manners and a good education.

One could say that organizations are becoming more “cultured” in the ways of good security practices, and are developing a broader perspective toward the topic than previously held.

*Published in Security Magazine, September 1, 2007.*

**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.**



800-843-4488 | [www.forsythe.com](http://www.forsythe.com)

© 2007 Forsythe Solutions Group, Inc. All Rights Reserved. Contents may not be reproduced, in part or in whole, without prior written permission from Forsythe.