Chapter 11
Information Security
by Words Alone:
The Case for Strong Security Policies

Kirk P. Arnett
Mississippi State University, USA

Gary F. Templeton
Mississippi State University, USA

David A. Vance
Olivet Nazarene University, USA

ABSTRACT
Effective information security extends beyond using software controls that are so prominently discussed in the popular and academic literature. There must also be management influence and control. The best way to control information security is through formal policy and measuring the effectiveness of existing policies. The purpose of this research is to determine 1) what security elements are embedded in Web-based information security policy statements and 2) what security-related keywords appear more frequently. The authors use these findings to propose a density measure (the extent to which each policy uses security keywords) as an indicator of policy strength. For these purposes, they examine the security component of privacy policies of Fortune 100 Web sites. The density measure may serve as a benchmark that can be used as a basis for comparison across companies and the development of industry norms.

INTRODUCTION
Daily reports of personal information losses provide a poignant reminder of what has become one of the top security issues for the American public. For citizens, the risks loom large regardless of the precautions that are undertaken. Strategies to protect our personal information appear in all major news media. As personal information safety risks grow, so does the abundance of media advertising, postal mail, and Web-based hints available to us as to how to best protect our personal information.

We rely on businesses that have access to our personal information to protect it, and unfortunately, the protection efforts of businesses commonly fail, and we see far too many stories relating the loss of masses of personal informa-
Information Security by Words Alone

tion in the military, government, business, and education. Undoubtedly, business, legislative, and personal efforts are underway that promise to strengthen protection efforts. One concern lies in how effective these efforts will be.

Following widely publicized data breaches at business behemoths AOL and AT&T, EWeek (2006) reports on a Ponemon Institute study stating that two-thirds of IT professionals claim to be ineffective at the prevention of data breaches. Recently, Seltzer (2008) questioned “Can you trust TRUSTe?” TRUSTe, an organization that provides symbols of trust on the Internet and serves as a guardian of the privacy protection policy enforcement for Web sites, has come under fire as a result of allowing, what appears to be, a significant breach of individual privacy when they certified Coupons, Inc. Coupons violated numerous privacy standards by hiding misleading named files in the registry and by creating misleading named files in Windows™ that store information about the computers on which they reside, yet maintained full TRUSTe certification. The open power of the Web has allowed creation of CVV2 (Card Verification Value 2) Web sites that sell others’ credit card numbers for different amounts depending on the amount of credit allowed on the card. In the legislative arena there have been several efforts aimed to encourage businesses to improve information and asset protection. Better known federal efforts include GLBA, HIPAA, and Sarbanes-Oxley, and there are also lesser known state laws as well. The Electronic Privacy Information Center (EPIC) presents the federal government’s effort to control corporate information privacy (see http://www.epic.org/privacy/bill_track.html for real-time updates on legislative efforts underway in the U.S. Senate and House). Individuals too are making personal efforts to better patrol the collection and use of their own information, and are rightly concerned about the efforts that business is making to protect personal information.

ADDRESSING THE PROBLEM

U.S. businesses have a strong interest in data protection and the efforts that are underway to protect the personal information of its customer community. From a business standpoint, policy is used to specify the company’s approach to security. Management selects and implements technology, but it is policy that guides and coordinates the selection and implementation of technologies. Security policy issues ranked sixth in an international survey of 874 certified information system security professionals (Knapp, Marshall, Rainer, and Morrow, 2006). There is no evidence that the importance of security policies should or will change in the foreseeable future.

Web-based security policies must reach beyond protecting against the threats of hackers and must extend to the causes of and solutions to insider threats. These Internal security breaches often result from worker stress brought on by organizational change or unpredictability. Events that may trigger internal breaches include “reengineering, downsizing, upsizing, mergers or acquisitions, rapid changes in markets or the economy, litigation, organized labor actions, and other traumatic phenomena” (Parker, 1996, p. 21). Although a company safeguards personal information from traditional hackers, there is evidence from the authoritative CSI Annual Security Survey respondents that more serious problems exist as “insider attacks edged out virus incidents as the most pressing security problem” (Richardson, 2007, p. 2).

Companies are sharing information with the public and communicating their protection efforts to the public, not only through Web site privacy policies, but also by U.S. mail, agreement forms, advertisement, etc. The flip side of this information sharing is that the public also has an interest in the policies that businesses are using for information protection. Some of these policies are widely available because they are posted on Web sites. But, as noted in a study of large U.K. organizations, although policies are common, there is consider-