Seeing both sides of the coin

Identity theft is a growing concern. ***Rodney Denno*** argues that user privacy measures lead to greater security.

Privacy and security are two key concepts in any serious discussion on the collection, use and protection of any organization 's information assets. Business runs on information. No one disputes that. What is in dispute now is who owns the information, how it is collected, used, stored, processed, shared, controlled (by the owner) and destroyed (when the owner wants it destroyed).

Information lives in a vastly different world from even 20 years ago. Firewalls, antivirus, intrusion detection and database access controls all separate information retained by individual organizations. Costs associated with collecting, retaining, processing and transmitting (to virtually any computer in the world) information no longer limit the amount of information an organization can collect. Hackers and malware have equal access to corporate web sites and networks, whether they are 'around the corner' or on the other side of the world. But organizations continue to think they own the information in the same way as they owned it 20 years ago.

Identity Theft Is Personal

In 1992, Trans-Union received about 35,000 calls about identity theft. In 2001, they received more than a million calls. A Florida grand jury estimated that average identity theft crime costs the business community about $17,000 per victim. Identity theft victim estimates for the U.S. during 2001 range from 700,000 to 1.1 million people.

At the low end, 700,000 victims equal losses of a staggering $11.9 billion. And this number does not include victim costs, including legal assistance, judicial and law enforcement time in investigating and trying cases. On average, victims spend 175+ hours and $1,000 in out-of-pocket expenses to clear their names. That's a lot of time, money and aggravation, not to mention the personal impact on real people's lives and aspirations.

Privacy Legislation

Globally, much of the privacy legislation that was being discussed five years ago is now either in effect or coming into effect over the next 12 to 18 months. Much of this legislation provides organizations with an operational and legal framework (for the first time in cyber-history) to plan, budget and implement appropriate technical and management solutions.

Results of surveys conducted in 2001 by the Federal Trade Commission indicated that although almost 90 percent of web sites post privacy policies, only about 20 percent meet FTC standards for adequately protecting consumer privacy.

The FTC proposed legislation that would allow it to implement and enforce "fair information protection principles." Developed as guidelines for industry self-regulation, these parallel the rules of fair-credit reporting. The principles include providing notice to consumers about the kinds of privacy policies followed by each web site, and allowing consumers access to the information that companies keep about them.

In April 2002 Senator Fritz Hollings introduced the *Online Personal Privacy Act* (S-2201). The bill is designed to safeguard inter net users' privacy while still allowing online businesses to collect personal information. This measure aims to create a national online privacy policy that would pre-empt individual state regulations.

The new bill divides personal information into two categories. 'Sensitive' data relates to a person's financial and health information, ethnicity, political and religious affiliation, sexual orientation and social security number. Online companies must obtain a consumer's clear consent — or have them "opt in" — before sensitive information is collected.

All other collected information — ranging from a web site visitor's address to preferences in purchasing books — would be considered non-sensitive information and would not require advance permission from the user to be collected. However, an online merchant would have to provide users with an "opt out" option if they did not want this information collected.

Business runs on information… What is in dispute now is who owns the information, how it's collected, used, stored, shared…

The bill would require that the opt-out option be accompanied by a "robust notice" displayed at the point that information is collected to inform the user of how non-sensitive data may be used by the on-line establishment.

In addition, online merchants would have to post "clear and conspicuous" notices detailing their policies for handling personal information, regardless of which category of data they plan to collect. Online consumers would be given the right to find out what information a web site has collected about them, similar to consumers' rights to detailed descriptions of their credit history. But only information collected after the bill is enacted would be subject to its rules.

The bill allows for user redress by granting consumers whose sensitive information was shared with- out their consent to seek damages in a federal court. The FTC, which already handles many privacy is- sues, would enforce the bill and would issue periodic reports on the measure's efficacy and whether additional steps to protect privacy should be taken.

A Federal Chief Privacy Officer?

The Bush administration is expect- ed to recommend appointing a federal chief privacy officer to act as watchdog. The federal CPO would have primary responsibility for vetting government data gathering and security initiatives for potential privacy problems.

The chief privacy officer would work in the Department of Homeland Security and would oversee a privacy advocate at each federal agency. The advocates would be responsible for facilitating an annual review of each agency's compliance.

A chief privacy officer as an integral part of the Department of Homeland Security will no doubt generate a lot of debate. It does however highlight the fact that privacy and security are two sides of the same coin. .

Rodney Denno, CISSP,
is president of Secure Open Systems Inc.
(*www.opensystemssecurity.com*)