Chapter 68
School Districts Stumbled on Data Privacy

Irene Chen
University of Houston Downtown, USA

ABSTRACT
The story describes how three school institutes are grappling with the loss of private information, each through a unique set of circumstances. Pasadena City Public Schools discovered that it had sold several computers containing the names and Social Security numbers of employees as surplus. Stephens Public Schools learned that personal information about students at one of its middle schools was lost when a bag containing a thumb drive was stolen. Also, Woodlands Public Schools accidentally exposed employee personal data on a public Web site for a short period of time. How should each of the institutes react?

BACKGROUND INFORMATION
Most parents know that school districts request information when:

- Registering for emergency announcements.
- Providing feedback in an online survey.
- Subscribing to a newsletter or a mailing list.

Parents allow schools to collect information including names, e-mail addresses, phone numbers, addresses, types of business, genders, dates of birth, behavior and assessment records, customer preference information, as well as other sensitive personal information. They collect, store and use the personal information of students and parents, for defined purposes. They use the information to provide service and support and share news and information with families and communities. We all assume that they strive to protect the security of personal data by use of appropriate measures and processes. More importantly, we also trust that they do not sell our personal information.

When talking about data security, most of us think of procedures and practices for data encryption, audit logging and incident handling, and secure remote access. However, some data