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

DOI: 10.4018/978-1-4666-4707-7.ch068

security incidents occur at the most unexpected moments and places.

Keeping data secure, safe, and legal is everyone's responsibility and needs to be embedded into campus culture and ways of working. Therefore, we encourage you to discuss data handling and information security and to give feedback after reading the three incidents below.

THE CASE

Three school institutes in the western United States are grappling with the loss of private information of students, parents, or employees, each through a unique set of circumstances.

Pasadena City Public Schools allowed the leak of personal information on about 650 employees as a result of auctioning surplus computers. The sale of six obsolete computers included hard drives containing names and Social Security numbers of district employees. The district dissemnated a letter to the employed and then posted the letter to the district's homepage outlining that standard procedures had not been followed with the sale of the Division's outdated computers, and that the hard drives from some of the outdated computers were not removed prior to the sale. Luckily, the district has since recovered the drives. The individual who purchased the computers signed a statement verifying that no material had been copied or disseminated. In an effort to further protect employees, the district took the following measures:

1. A letter with more detailed information was sent to affected employees.
2. A hotline was created for employees to call with questions/concerns. The hotline was available within 36 hours of the release of the news and the number included in the letter.
3. Free credit monitoring services were provided to affected employees.
4. The Division would work closely with the City Police Department to provide assistance to employees.
5. The district was reviewing existing protocols and implementing additional procedures to prevent future incidents.

In the case of Stephens Public Schools (student population 1,600), parents of students at Wake Lake Middle School (student population, 1,600), received a letter from its principal in September regarding the theft of confidential school division data. The data was maintained on a thumb drive taken off school property for the sake of emergency backup and was in a bag taken during a burglary off campus. The data included student identification numbers, student names, parent/guardian names, parents' cell, home, and work phone numbers, and student bus numbers or walker status. Additional "identifiable data" might also have been recorded. The school held an informational meeting to answer questions from concerned parents. Two assistant principals of the school were assigned to handle in-coming phone calls and media attention.

The district posted the information in Table 1 on its homepage to inform the community.

Not long after the above incident happened, Woodlands Public School learned that it had posted on a Web site, encrypted personal information about some employees, including names, home and work addresses, and individual employee pay scales. The data was contained in a spreadsheet outlining proposed budget cuts for the next academic year. The spreadsheet was e-mailed to an external consulting company that was hired to assist with budget calculation and was posted on a Web site.

Even though the file had been deleted and is no longer available on the Internet, the school department was urging employees to be alert to the possibility of identity theft.

In a memo sent out to the employees, the Superintendent warned that the information was