



Eliminating Personal Identity Theft Exposure at Colleges and Universities

White Paper

Published: August 5, 2005

Produced by:

twentysix New York
a business solutions provider

62 West 45th Street
New York, NY 10036

www.26ny.com

Introduction

Almost every week there is a front-page article about another case of large-scale personal identity theft. Many of these involve universities and colleges.

Within the past month, a programming error in the University of Southern California's online system for accepting applications from prospective students left the personal information of users publicly accessible.

According to the person who discovered the vulnerability, the flaw put at risk hundreds of thousands of records containing personal information, including names, birth dates, addresses and social security numbers. The Web programming error allowed the person, who asked only to be identified by the alias, 'Sap', to slip commands to the site's database through the log-in interface.

Why are security breeches like this happening?

Emerging market for personal identity information

With the advent of the information age and the use of the Internet for shopping, paying taxes and accessing bank accounts, individuals have been transformed into data that represents their identity.

This data includes:

- Social Security numbers (SSNs)
- Full name and date of birth
- Credit card numbers
- Bank account numbers and more

Such data elements have become our personal identifiers (PIDs) and represent us to the multitude of information systems that support financial and other transactions.

As a result, there is an emerging global market for these personal identifiers, which allow criminals to impersonate individuals. These criminals can go on a shopping spree, set up utility company accounts, rent homes, create and access bank accounts with such a small amount of information. A person's name and SSN is estimated to be worth three to five dollars in this market. Add a credit card number and expiration date and the value jumps to ten dollars. Suddenly, a class roster or faculty list containing SSNs and a filing cabinet of alumni credit card contributions look like a goldmine to those interested in taking advantage.

Educational institutions are easy targets

Colleges and universities are in the business of education, and that business is all about people – teachers, students and administrators -- and their identities. Individuals become students by applying and being accepted for admission. Early in the admission process, SSNs are used for identification and eventually can be linked to test scores, transcripts, as well as loan and scholarship applications.

New professors applying for staff or faculty positions are identified by SSNs. Grant requests and recipients are referenced by SSNs. Additionally, there is the standard SSN requirement for employee benefit and tax purposes.

Colleges and universities also solicit contributions from parents and alumni members who are identified by SSNs. Contributions are charged to credit card numbers that can be obtained by mail, phone or electronically. The records of these transactions are required to be retained for tax purposes and additional solicitation.

Traditionally, the information technology (IT) department at these educational institutions has evolved from a small group of part-time student employees to become a critical component of today's educational business. Security concerns are new to a culture that values its openness and availability of information.

The cost of theft

The cost of identity theft to colleges and universities has become large enough that in many cases the current approach to using personal identifiers and the surrounding culture needs to change.

Individual students, faculty staff, or administrative employees that have had their identity stolen can suffer large personal financial loss. Clearing up their finances and credit history and recovering their stolen identities is a process that can take many months, if not years.

When identity theft takes place, educational institutions absorb the cost of informing the victims. If the theft involves parents or alumni, relations that have taken years to form can be broken and then take years repair. If the institution has been careless in safeguarding personal information, it is at risk for law suits.

Personal identity security analysis

A Personal Identity Security Analysis is not concerned with computer database or network security. Instead it is a process that identifies a school's exposure to identity theft and recommends actions to limit that exposure. One or two business analysts can accomplish this in a two- to four-month time period.

The analysis identifies physical internal and external information flows that contain personal identity information. The flows are classified as required or not required, and can also be characterized by the physical media involved – for example an Internet transaction, tape, CD or paper – as well as their sources or recipients.

In addition, there are several by-products of this analysis:

- Overall business processes are frequently simplified
- Unnecessary or incomplete flows are clarified and can be eliminated
- Unneeded business processes are discovered

The resulting report details these findings and recommends actions to be taken to reduce or eliminate the potential for identity theft.

The sponsors also receive diagrams representing the information flows and business processes analyzed. This information and the resulting flow categorizations are left in a database of the sponsors' choosing. The On-Line Analytical Processing (OLAP) cubes and charts used for the quantitative analysis are also available, if requested.

Conclusion

Over half of this country's universities and colleges still use SSNs and other personal information as a form of identification, potentially putting faculty and students at risk.

In order to secure personal data, and meet current and pending compliance regulations, schools need to uncover potential risks and exposures that they might not have been aware of. Initiating a Personal Identity Security Analysis is a proven way to meet that challenge.

twentysix
NEW YORK