Cards at School

Why Banks View Campuses as High Risk Customers

Dennis W. Reedy, CTP, Managing Director, Treasury Operations, Indiana University
Walter Conway, Walter Conway Associates, LLC

Accepting credit and debit cards is a fact of life at campuses nationwide. Hand-in-hand with card acceptance comes the responsibility to safeguard and protect all transaction and consumer data. The Payment Card Industry Data Security Standard (PCI DSS) was created to help ensure the safe handling of sensitive consumer payment information.

While PCI DSS applies to every organization that accepts payment cards, many education institutions have been slow to achieve campus-wide compliance. This situation is particularly unfortunate since education institutions—whether because of their open networks or inadequate security procedures—are particularly vulnerable to hacking and other compromises of confidential consumer data. As a result, financial institutions and card issuers increasingly view education institutions as risky merchants.

Below, in addition to a description of PCI DSS, there is data analysis from nearly 500 publicly reported computer security breaches to quantify the case that compliance with the standards, while a business fact of life, is also good practice for every campus.

What is PCI DSS?

The Payment Card Industry Data Security Standard represents a common set of technical requirements and testing methodologies created to help ensure the safe handling of sensitive information. It was initially created to align the separate security programs of MasterCard and Visa, and later was adopted by other major card programs. In 2006, the PCI Security Standards Council was created to govern the security standards for the payment industry. Founding members of the council included American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

According to the council: "The PCI DSS is a multi-faceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures." In practical terms, the PCI DSS is a set of 12 general requirements grouped into six areas: build and maintain a secure network; protect cardholder data; maintain a vulnerability management program; implement strong access control measures; regularly monitor and test networks; and maintain an information security policy.

There are two things treasury managers at every education institution need to understand about PCI DSS. The first is that the standards are not optional—if you accept payment cards anywhere on your campus, you are subject to the standards. The second thing to understand is that there can be significant financial costs to non-compliance.

For example, if your institution suffers a security breach and cardholder information is compromised, there are potential direct costs (e.g., notifying affected cardholders, paying for credit monitoring, paying for unauthorized charges, implementing needed hardware or software upgrades) and indirect costs (e.g., unfavorable publicity, brand damage to the institution) resulting from a breach. In addition, your institution may be fined by the card association(s) whose cardholders were affected. It is worth noting that in 2006, Visa alone issued merchant fines totaling $4.4 million[1].

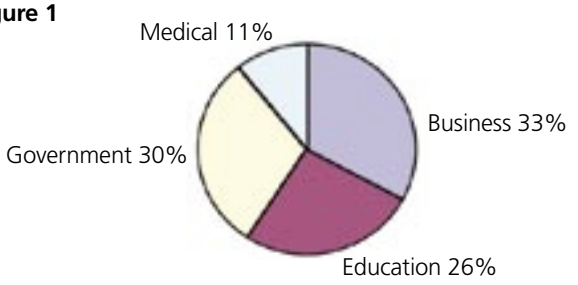
Education institutions are disproportionately vulnerable to security breaches

There were 321 publicly reported computer security breaches in the United States in 2006[2]. The 321 breaches are described in Figure 1 and graphically displayed in Figure 1.

Table 1

- 106 were at businesses
- 84 at education institutions
- 96 at government agencies (state, local, and federal)
- 35 at medical institutions (hospitals)

Figure 1



Analyzing this data, we see that education faces an acute problem: 26% of all reported security breaches in 2006 were at education institutions. The share for businesses was 33%. The percentage for education is disproportionately large given that:

- There are vastly fewer education institutions than there are businesses (D&B lists over 14 million businesses in the U.S.[3]); and
- Education institutions deal with a small percent of the total population and conduct a very small share of all financial transactions.

The picture does not change when we look at the total database of 498 security breaches since 2000. Over that period education's share of security breaches was 32%, nearly equal to the 35% for business.

Other studies[4] confirm the conclusion that education institutions are particularly vulnerable to security breaches. For one thing, college and university databases are attractive targets since they contain sensitive data such as names, addresses, Social Security numbers, and credit card transaction information. At the same time, education institutions have open networks to support their education mission.

Compounding these two factors is the frequent lack of internal controls enforced throughout campus that could limit vulnerability. An example is the 2003 hack at a West Coast university that compromised 200,000 Social Security numbers. According to a university spokesperson, the hacker "wiggled his way through an outdated system in the drama department to reach the financial aid system.[5]" The combination of valuable private data and lax controls presents an attractive target for outside hackers and malicious insiders.

At this point it is imperative to recognize that information loss is not the same as identity theft. Ergo, sometimes a thief wants only the PC and not the sensitive data that may be stored on it, and a misplaced computer tape can end up buried in the dump. However, once personal data are compromised (or worse, published or offered for sale on the Web) they are lost forever. Personal information like names, birthdates, and social security numbers do not change. This means identity theft is like a time bomb that may not explode today, but the risk and vulnerability never goes away[6].

Education institutions are particularly vulnerable to hacks

We can classify security breaches by five sources:

- Fraud (e.g., phishing)
- Improper disposal of media (e.g., paper records not shredded or destroyed)
- Hacking into networked computers
- Lost or stolen PCs and storage media
- Other (e.g., mistakenly posting of confidential information on the Web).

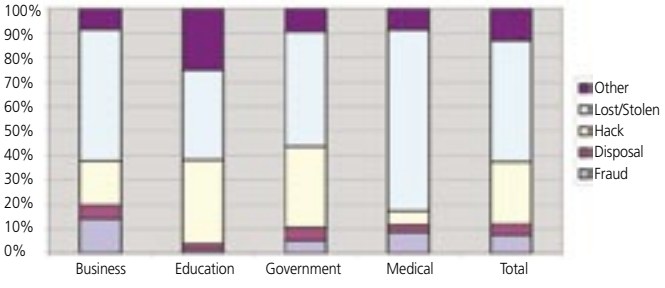
Table 2 analyzes the experience of each industry by type of security breach. Figure 2 graphically compares each industry by looking at the percentage of breaches attributable to each source.

This data tells two stories. First, the largest source in terms of number of security breaches is lost/stolen PCs and media.

Table 2

Type of Breach	Business	Education	Government	Medical	Total
Fraud	15	1	5	3	24
Disposal	6	2	5	1	14
Hack	19	29	32	2	82
Lost/Stolen Computers and Media	57	31	45	26	159
Other	9	21	9	3	42
	106	84	96	35	321

Figure 2



This conclusion holds across industry. But there is a second, possibly more important, story for educational institutions.

Together, hacking and lost/stolen PCs account for roughly three-quarters of educational security breaches. This is about the same share as businesses and for the U.S. as a whole. What is different for those focused on education, however, is the significance of hacking incidents (both number and percent) at these institutions. Based on the 2006 experience, 35% of education breaches were due to hacking. This is roughly twice the percentage as for businesses (18%) and significantly higher than the total for all other industries (20%). The data for the longer period 2000-2006 show a similar pattern.

This observation is not meant to imply that lost/stolen PCs are not a significant source of information security breaches. As we saw, in absolute numbers there are more breaches due to lost/stolen PCs than to hacking. Rather, an equally or possibly more significant conclusion is that the percentage of educational breaches due to hacking is significantly out of line with the experience of other industries. As we discussed above, while the hardware itself may be the primary motivation in the case of a stolen PC, in the case of a hack the objective is most often access to the sensitive personal data compromised. This makes hacking a much more serious threat.

Sensitive personal information is compromised

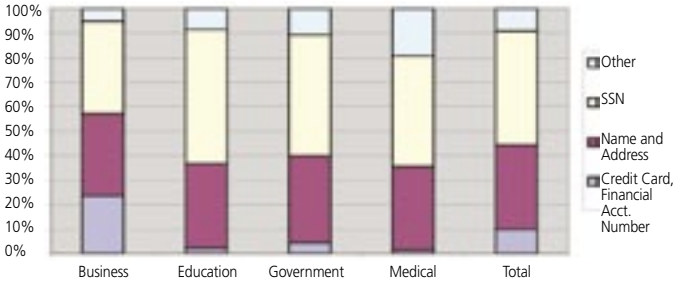
Table 3 contains data describing the types of data compromised or lost by industry. The data are graphically displayed in Figure 3.

Ninety percent of education breaches involve Social Security numbers or names and addresses, a result that is roughly

Table 3

What Gets Stolen	Business	Education	Government	Medical	Total
Credit Card, Financial Acct. Number	24%	2%	4%	2%	10%
Name and Address	33%	35%	35%	34%	34%
SSN	38%	55%	49%	45%	46%
Other	5%	9%	11%	19%	9%
	100%	100%	100%	100%	100%

Figure 3



consistent with other industries. We also observe that only 2% of education breaches involved financial information such as credit card numbers, a figure that is much lower than the 24% of business breaches that involved financial records.

While 2% may seem low, education institutions still need to comply with the PCI DSS in the same way they must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other mandates. What our analysis points out is the broad need for greater emphasis on protecting all personal data entrusted to the institution including Social Security numbers, names, addresses, e-mail accounts, medical records, and payment information.

Education breaches generally involve fewer accounts

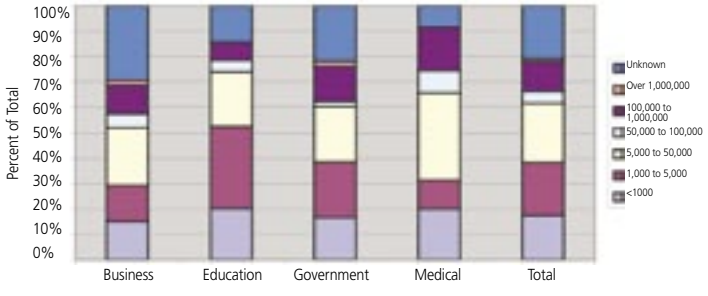
Table 4 contains data on the relative size of security breaches for each industry. These data are represented graphically in Figure 4.

Looking at Figure 3, we see that over 50% of education breaches involved less than 5,000 accounts (20% involved less than 1,000). The comparable figure for businesses is 29% and for all industries it is 38%. Additionally, where 13% of business breaches involved more than 100,000 accounts, only 7% of education breaches were this large. Data for the longer period 2000-2006 are consistent with this pattern.

Table 4

Number of Accounts Compromised	Business	Education	Government	Medical	Total
< 1000	16	17	16	7	56
1,000 to 5,000	15	27	21	4	67
5,000 to 50,000	24	18	21	12	75
50,000 to 100,000	6	4	2	3	15
100,000 to 1,000,000	12	6	13	6	37
Over 1,000,000	2	0	2	0	4
Unknown	31	12	21	3	67
	106	84	96	35	321

Figure 4



While having a security breach of several thousand accounts is still serious, and there were several very large security breaches at education institutions in 2006 (including at least six with over 100,000 accounts compromised), it generally appears that security breaches at education institutions tend to be on the smaller side. Nevertheless, the costs of any breach can be substantial, and they include:

- Direct financial liabilities (e.g., costs to notify consumers, paying for credit monitoring, potential liability for card reissuance and unauthorized transactions, and fines levied by card issuers or their associations)
- Indirect costs (e.g., forensic analysis, system upgrades, management time and attention)
- Brand damage (e.g., bad publicity that sours student, parent and alumni relations).

Conclusions

Utilizing a database of 498 publicly reported computer security breaches from 2000 to 2006 to try and understand why banks and financial institutions may view campuses as risky customers, the following was observed:

- Colleges and universities appear to be disproportionately vulnerable: while relatively few in number, education institutions account for more than a quarter of all reported security breaches. We can only speculate as to the reasons, but pos-

Continued on page 31

Cards at School *continued from page 29*

sible explanations include the combination of large amounts of valuable personal and financial data, open networks, and lax internal controls across campus departments.

- While the most frequent form of security breach is lost or stolen PCs and storage media, campuses are twice as vulnerable to hacking and other outside attacks as businesses.
- The most frequently compromised data are Social Security numbers and names and addresses. These fields (especially combined with a birth date) are an identity thief's toolbox.
- Half of education security breaches involve 5,000 or less accounts—a large number to be sure, but smaller than we found with business breaches.

We conclude that in this context, PCI DSS compliance should remain a high priority for college and university financial managers. PCI DSS compliance can help protect institutions from the very real financial costs and brand damage that accompany any security breach. Therefore, compliance is not only necessary, it is a good investment.

Postscript

The Treasury Institute for Higher Education sponsored a two-day workshop in May 2006 to share common experiences, lessons learned, and insights among educational institutions. The workshop attracted 89 professionals from institutions nationwide and featured energetic discussion and information sharing among participants. Recognizing the continuing need to share best practices and remain current—PCI DSS was revised in July of 2006—the Treasury Institute is again sponsoring a workshop in May 2007. The Institute's Web site (www.treasuryinstitute.org/welcome/) contains additional information on this workshop including online registration.

Footnotes:

1. Visa News Release, December 21, 2006
2. Source: Attrition.org (http://attrition.org), a computer security Web site dedicated to the collection, dissemination and distribution of information about the industry. Attrition provided the open source database, which was loaded into an Excel spreadsheet for editing and analysis.
3. Source: Dun & Bradstreet
4. The New York Times (December 18, 2006, "An Ominous Milestone: 100 Million Data Leaks") reported on a study by the Public Policy Institute for the AARP in July 2006, using data compiled by the Identity Theft Resource Center, determined that of the 90 million records reportedly compromised in various breaches between January 1, 2005, and May 26, 2006, 43% were at education institutions.
5. "College Door Ajar for Online Criminals," Los Angeles Times, May 30, 2006.
6. "Black Market in Stolen Credit Cards Thrives on the Internet," New York Times, June 21, 2005
7. For example, see "More Holes than a Pound of Swiss Cheese", The Chronicle, September 29, 2006