

How Safe Are We in Our Schools?

Joseph E. Campana, Ph.D., CIPP/G, CITRMS
J. Campana & Associates LLC
PO Box 70726 ■ Madison, WI 53707
608-241-3500 ■ www.JCampana.com

Latest Revision: November 12, 2008

How Safe Are we Safe in our Schools?

Executive Summary

Results

Education-related organizations account for nearly one-third, 31%, of all the data breach incidents reported in U.S., although the Education Sector makes up 0.6% (at least) to 13% (at most) of all entities in the U.S.

Education-related organizations reported more than 12.4 million student and consumer profiles have been compromised in 324 breach incidents, which account for more than 25% of all profiles compromised through “*typical*” information security breaches.

12.4% of all reported education-related breach incidents did not specify a numerical value as to the number of student and other consumer profiles that were compromised. For example, one of 12.4% was characterized as, “Tens of Thousands,” while all others were characterized as *unknown*.

Institutes of higher education account for 79% of all education-related breach incidents and for 78% of all of the compromised consumer profiles reported by Education Sector.

K-12 schools comprised 15% of all reported breach incidents by the Education Sector, although K-12 breach incidents account for just 2% of all the total profiles compromised by the sector. K-12 schools also reported the largest percentage (30%) of breach incidents where the number of profiles compromised was characterized as *unknown*.

Of the breach incidents reported by the Education Sector, at least 24% were characterized as resulting from a **Hack Attack** on information systems. Many more simply characterized the breach as resulting from “unauthorized access,” which may include intrusion by a hacker.

Over a third (35%) of the breach incidents were characterized as involving lost, stolen, missing, or improperly disposed computers, electronic storage devices, magnetic tapes, paper files and microfiche. Such breach incidents involving electronic storage devices accounted for 32%; “laptop-only” accounted for 15%; and traditional files (paper, microfiche) accounted for 3%.

Conclusions

The number of data breach incidents and profiles compromised by educational institutions is disproportionately high compared to the total of all other U.S. enterprises that reported data breach incidents.

Breach incidents in the Education Sector reported by K-12 institutions are disproportionately low (15%) compared to those reported by the higher education category (79%) recognizing that there are more than 20 times the number of elementary and secondary schools compared to postsecondary institutions. This observation suggests that K-12 institutions may not be detecting or recognizing data breach incidents when they occur and may not be reporting data breach incidents when they are recognized.

The large number of breach incidents that described the number of records compromised as *unknown* suggests that many schools do not keep an inventory of personally identifiable information that they maintain.

Recommendations

Schools should invest in mandatory awareness education that includes all faculty, staff and students. Awareness education is relatively inexpensive yet highly effective in getting faculty and staff to safeguard sensitive information and to recognize risks and incidents where sensitive information may be compromised.

Schools should invest in data encryption utility software. Contrary to common beliefs, data encryption utilities are inexpensive, simple and easy to use. All personally identifiable information that schools and related service organizations maintain in electronic form should be encrypted.

Schools should contractually require all business associates (vendors, support organizations) with whom they share their constituent's personally identifiable information to maintain a privacy and information security best practices program and to comply with all applicable laws requiring the safeguarding of personally identifiable information.

Introduction

Most every American is in a school at this very moment. Schools house our most precious asset, our identity—24/7, in the form of paper and electronic records. Whether you have children in school or you are currently a student, an alumnus, a parent, a teacher, a staff member, a donor, a volunteer or other patron, schools maintain our identity in the form of our name, birth date, Social Security number, health and medical records, credit card account numbers, student ID numbers, educational records, and other personally-identifiable information. Over 85% of all adults 25 years and older have completed at least high school¹ suggesting that their personal identifiers are housed in at least one primary and one secondary school location, if not also in a middle school and an institute of higher education.

How safe is the personally identifiable information that we entrust to our schools?

Method

Data breach incidents that have been reported to and compiled by the Privacy Rights Clearinghouse² from January 2005 through October 2008 (*A Chronology of Data Breaches*) were reviewed, interpreted and compiled for this semi-quantitative analysis of Education Sector data breach incidents. Entries in the *Chronology of Data Breaches* were reviewed and categorized into one of three Education Sector categories depending on the entity that was in control of the data when the breach incident occurred:

1. **K-12** institution (schools and school district offices)
2. Institutes of **Higher Education** (colleges, universities, and technical schools)
3. **Others** (such as service providers, student loan entities, regulatory agencies, etc.)

The data in the Privacy Rights Clearinghouse *Chronology of Data Breaches* includes

- (a) The date the breach incident was made public;
- (b) The name and location of the entity responsible for the data compromised (the data controller), in some cases the data controller reported a third party (e.g. a vendor) that was in possession of the information when it was breached;
- (c) A “free form” description of the breach; and
- (d) The number of records (or individual profiles) that were compromised, if known.

It was not unusual for (c) the description to contain a few words, for example, “Hacking,” or “Stolen Laptop;” although reports that are more current tended to provide content that is more descriptive. It is also not uncommon for (d) the number of records to state **unknown**. One of the challenges of interpreting these data is the unstructured or *free-form* nature of the data breach incident description.

For the reporting period of January 2005 through October 2008, all 1,033 breach incidents were considered for this study. These breach incidents account for over 245 million consumer profiles or records that were compromised.

The Privacy Rights Clearinghouse obtains information about security breaches primarily from The Open Security Foundation list-serve (www.datalossdb.org). It has been speculated that potentially thousands of data breach incidents go unreported or undetected monthly³, especially by smaller enterprises including businesses, not-for-profits, local government, and schools. Although we postulate that the *Chronology of Data Breaches* significantly under report the true number of data breach incidents that have occurred in the U.S.; it is the most comprehensive list of known data breach incidents that has been compiled.

Results and Discussion

Figure 1 illustrates that almost one-third of all breaches reported involved the Education Sector.

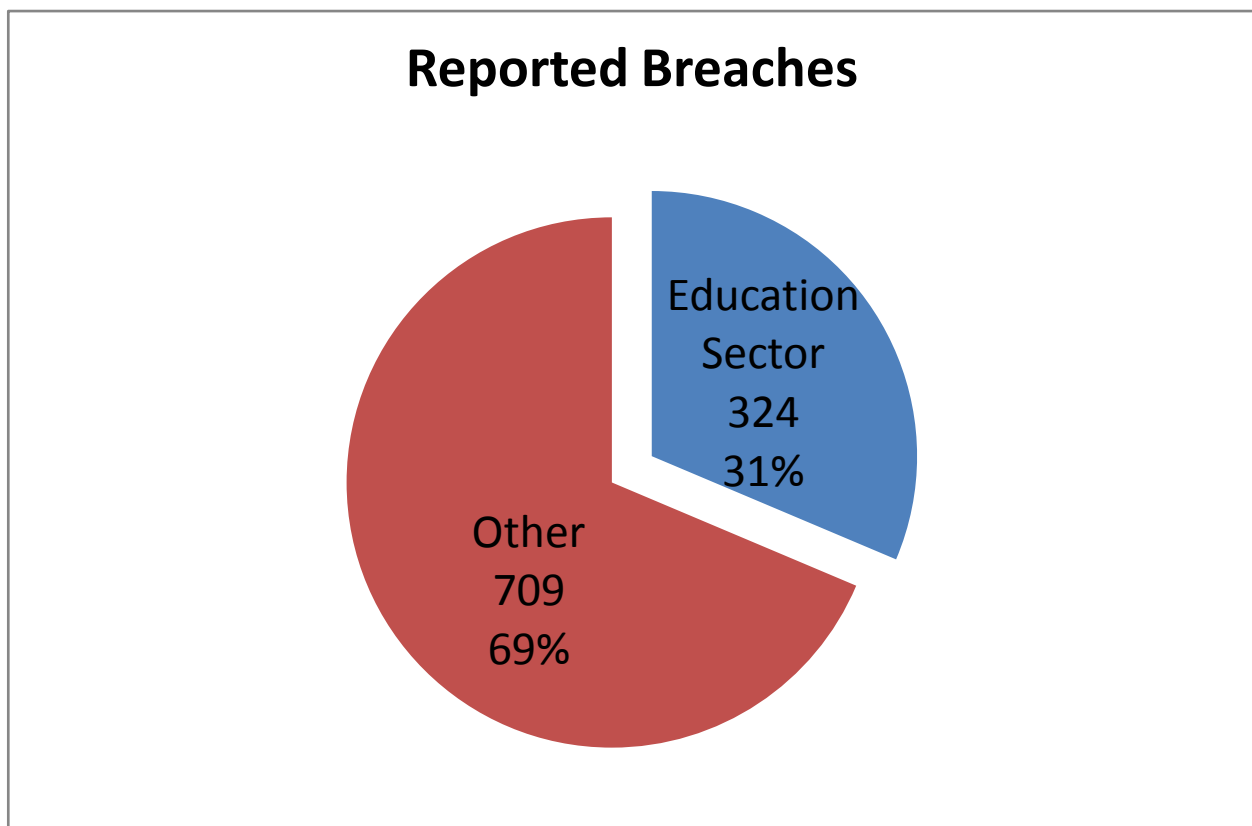


Figure 1. Comparison of data breach incidents reported by the Education Sector compared to all others reporting during the period of January 2005 through October 2008.

Nearly 250 million consumer profiles of Americans have been compromised in breach incidents reported during the period January 2005 through October 2008. Of these, the Education Sector breach incidents

accounted for at least 12.4 million (41 incident reports stated that the number of profiles breached were **unknown**).

Figure 2 illustrates that a significant number of the total profiles compromised (69%) resulted from a few Mega Breaches in other sectors (Retail, Financial and Government): TJ Stores (over 100 million accounts), CardSystems (40 million accounts) and the U.S. Department of Veteran Affairs (28.6 million veterans).

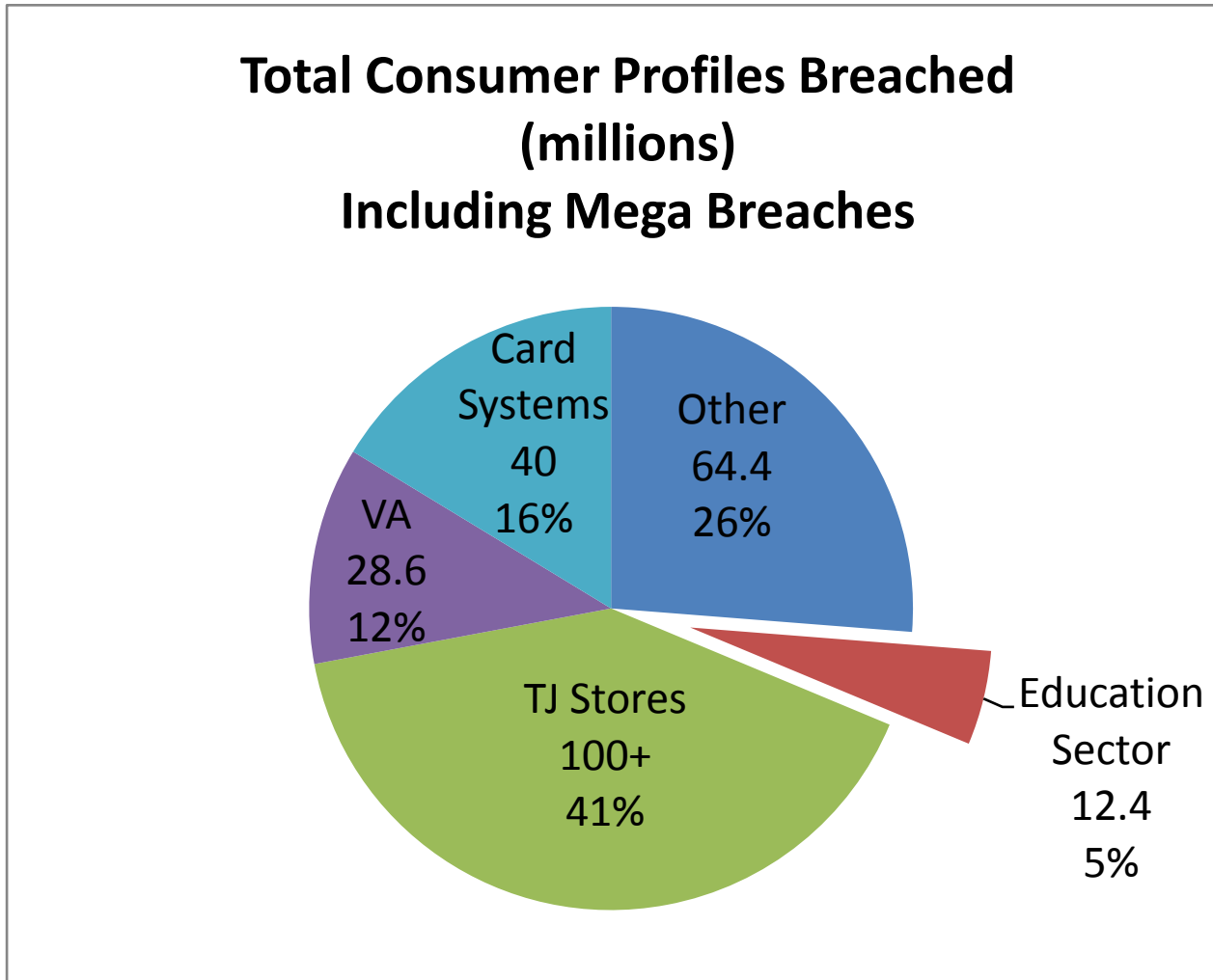


Figure 2. Total American consumer profiles that have been compromised in all reported data breach incidents. Mega Breaches by TJ Stores, CardSystems and the U.S. Department of Veteran Affairs (VA) contribute to nearly 70% of the profiles that have been compromised.

By comparison, the largest data breach incidents in the Education Sector involved the compromise of patient information: University of Utah Hospitals (2.2 million) and The University of Miami Medical School (2.1 million), followed by the Texas Guaranteed Student Loan Corporation (1.7 million). Only nine of all the reported breach incidents exceeded 2.5 million profiles.

One may view some or all Mega Breach incidents as anomalous data that could be excluded from consideration in order to obtain a sense of an average data breach incident. Figure 3 illustrates the comparison when the data from nine Mega Breaches, each exceeding the compromise of 2.5 million profiles each, are excluded. We chose 2.5 million profiles as one example because it was in the upper limit of the maximum profiles breached by educational institutions. Of this subset, Educational data breach incidents account for 25% of the total profiles breached in 1,024 reported incidents that exclude the nine largest Mega Breach incidents.

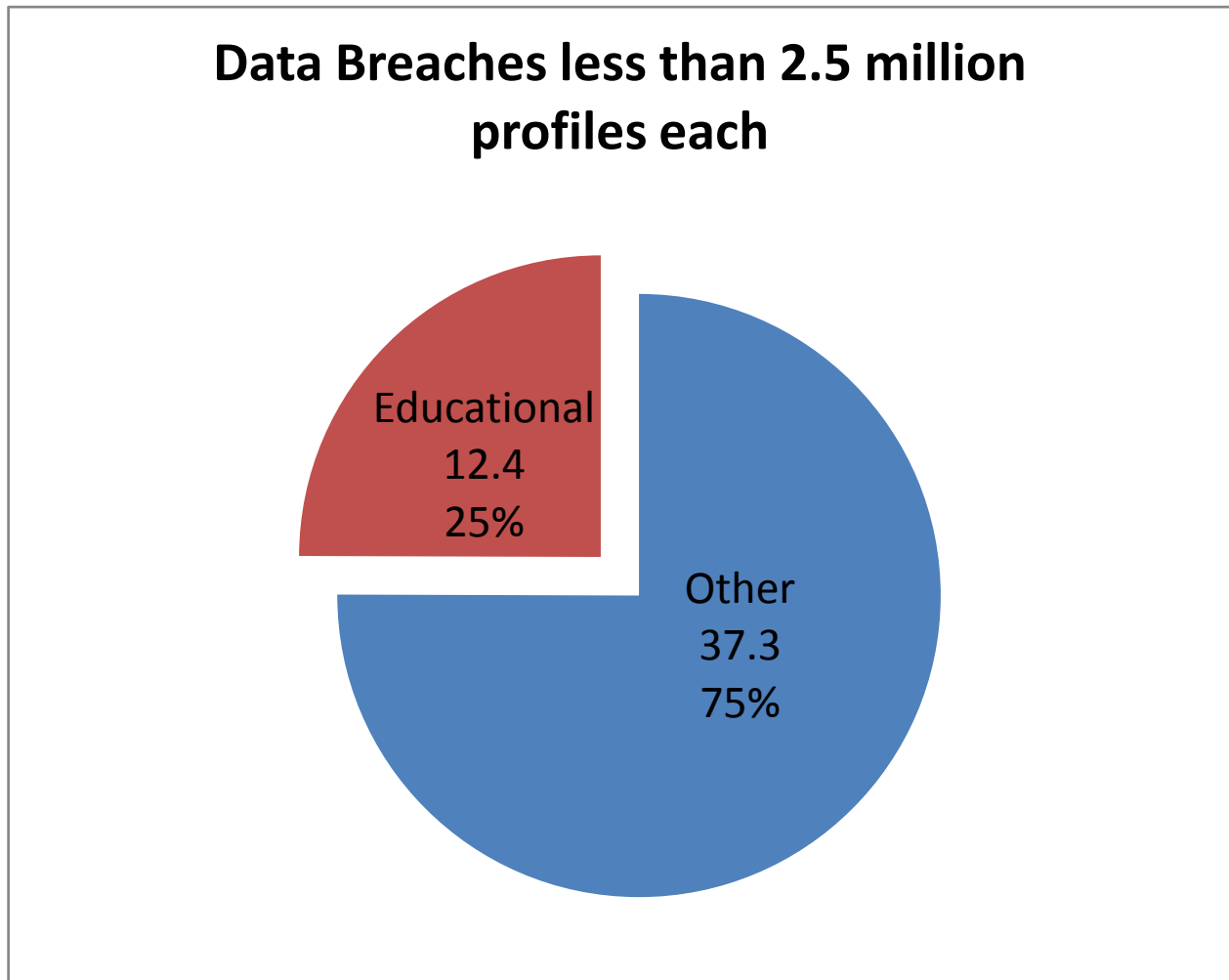


Figure 3. Education Sector data breach incidents compared against the total other breach incidents that reported the compromise of less than 2.5 million profiles per breach incident. These data correspond to 1,024 total breaches. Forty one (12.4%) of the Education Sector breach incidents reported that the number of profiles compromised was unknown. These unknowns may account for a significant number of profiles. One description simply characterized the number of profiles breached as “tens of thousands.” The average number of profiles compromised per breach incident by the Education Sector was 38,200.

Taking this “middling” or “average representation” of the reported breach incidences one step further by excluding all 22 Mega Breach incidences (breaches reporting the compromise of one million or more profiles) from both the Education Sector and other industry sectors provides results as a percentage that

are comparable to those illustrated in Figure 3: Educational 21% (6.4 million profiles) and Other 79% (24.2 million profiles).

A conclusion is that educational institutions have contributed to the compromise of a significant number of consumer profiles (up to 25% of the total) after excluding several of the exceptional (anomalous) Mega Breach statistics from the overall database.

Based on census and other statistical data^{4,5,6,7} educational enterprises comprise 06.1%–13% of all U.S. enterprises, yet they contribute to nearly one-third of all reported breach incidents and to as much as 25% of all profiles compromised (excluding incidences that reported 2.5 million or more profiles—Figure 3).

Current census data report that there are over 5 million businesses with employees⁴, approximately 20 million without employees⁴, and there are 1.5 million non-profit organizations⁷. Using the census data reported in References 4-7, the Education Sector is found to compose 0.6% of all enterprises in the U.S. This figure may be the accurate number to consider. If this value is considered to be appropriate, it should raise significant concern and alarm because it suggests that the Education Sector, which makes up 0.6% of all U.S. enterprises accounts for 31% of all reported breach incidents, 5% of all reported consumer profiles that have been compromised; 16% of all consumer profiles compromised excluding the three major Mega Breaches; 25% of all consumer profiles compromised excluding nine Mega Breach incidents reporting more than 2.5 million profiles each; and 21% of all consumer profiles compromised excluding all Mega Breach incidents (one million profiles or more) from consideration. This may be considered the “worst case” scenario, and it does not account for the 12.4% Education Sector data breach incidents that reported that an **unknown** number of profiles were compromised.

Many of the types of enterprises reported in the overall census numbers are not the types that are reporting data breach incidents or they are not capable of a breach incident, for example non-reporting not-for-profits, businesses with no employees, holding companies, inactive small businesses and inactive non-profits. In order to get a different picture, a best case scenario of how educational institutions compare to other *average* enterprises that have reported data breach incidents, we excluded certain types of business and non-profit organizations from the total number of enterprises. In this scenario, the Education Sector composes 13% of all U.S. enterprises. The result is illustrated in Figure 4. For this illustration, businesses with 20 or more employees were included in the business category, and reporting public charitable non-profits and operating private foundations were included in the non-profit category.

The trend illustrated by comparing Figures 1, 3 and 4 should be cause for concern. They suggest that the Education Sector, even when potentially overestimated by a factor of more than 20 (13%/0.6%) as consisting of as many as 13% of all U.S. enterprises, accounts for 31% of all breaches and 25% of all consumer profiles compromised after excluding the nine largest Mega Breach incidents.

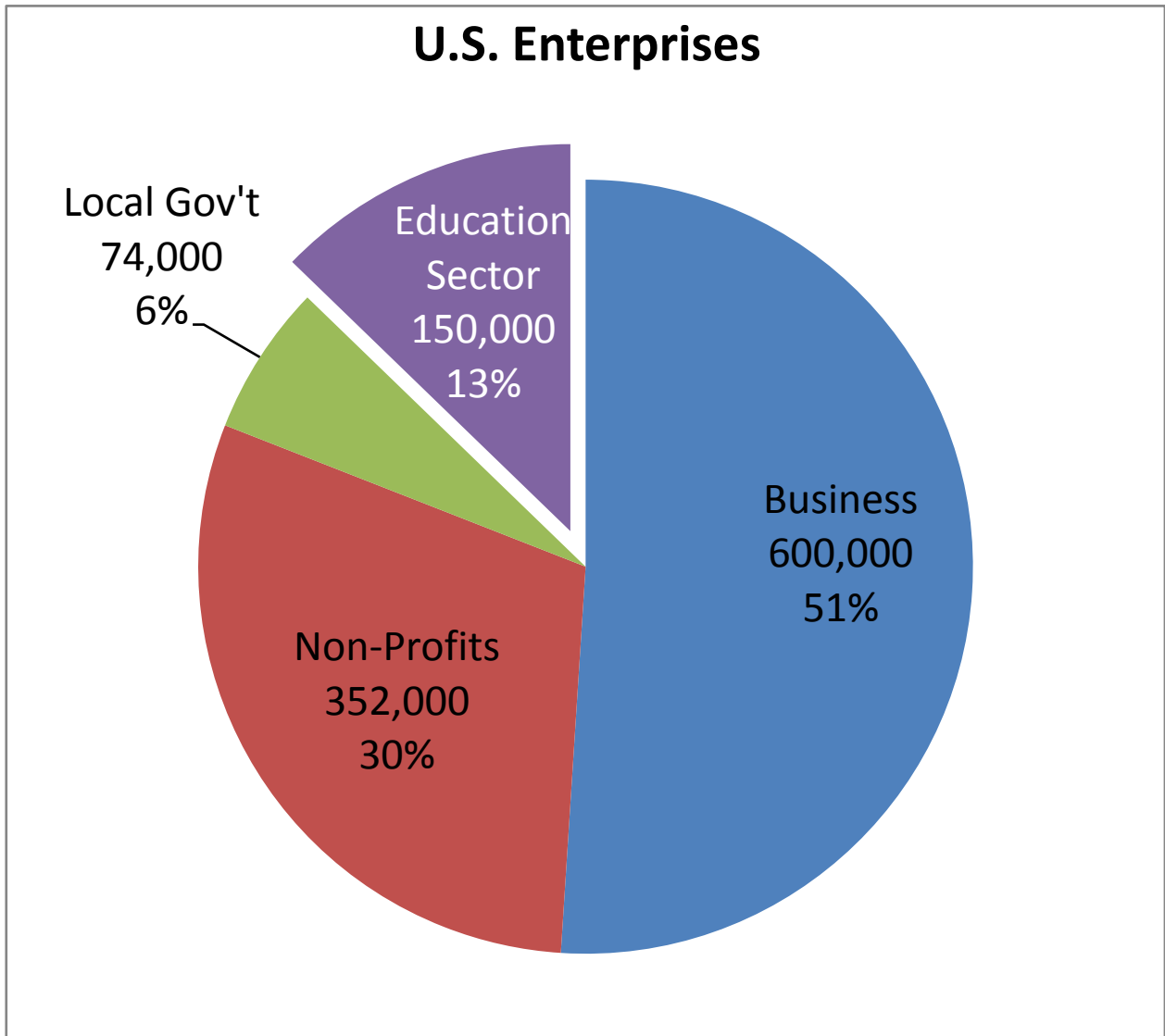


Figure 4. Educational institutions include public and private elementary schools, secondary schools, school districts and institutes of high education; Business includes only those businesses with 20 or more employees, and non-profits only include reporting public charitable and operating private foundations.

Figure 5 illustrates the total number of breach incidents in each Education Sector category (K-12, Higher Education and Other), and Figure 6 illustrates the number of profiles compromised per category. Each category reported breach incidents in which the number of profiles breached was characterized as **unknown**. K-12 reported the highest percentage of **unknown** (30% of all breach incidents were characterized as an unknown number of profiles compromised), followed by Other (14%) and Higher Education (9%). **Unknown** suggests that the organization does not have an accurate accounting of their information assets.

There are over 130,000 elementary and secondary schools in the U.S., and approximately 6,400 postsecondary institutions⁶. These statistics suggest that because the ratio of K-12 to postsecondary schools is 20:1 that the ratio of breach incidents reported by each would be in a ratio of 20:1; yet the ratio is less than 1:5.

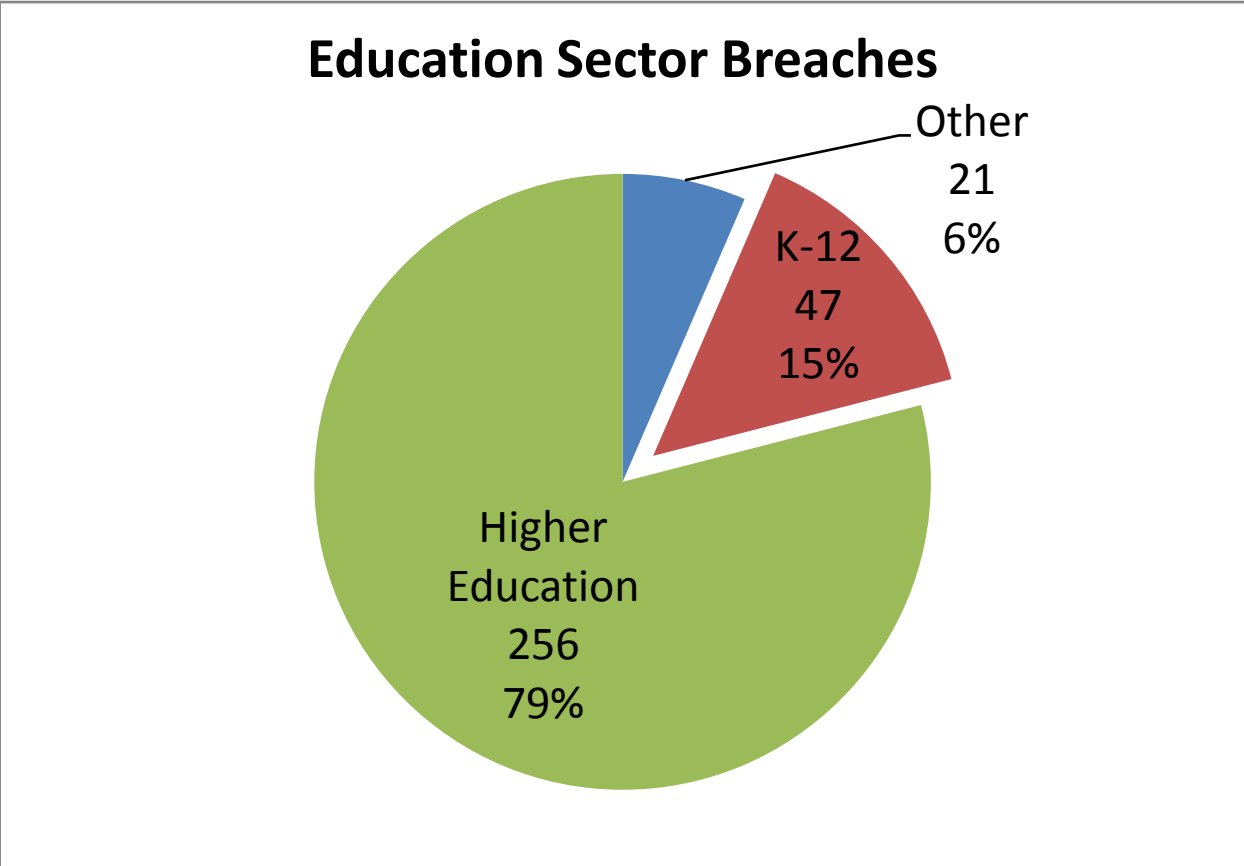


Figure 5. Number of data breach incidents by each of the three Education Sector Categories: K-12, Higher Education and Other (service providers and some regulatory agencies).

Some possible interpretations are of the disparity are:

1. K-12 schools have better privacy and information security compliance programs than postsecondary schools;
2. K-12 schools do little or nothing by way of acquiring, storing, or disposing of sensitive information—in other words there is little or no sensitive information to compromise; or
3. K-12 schools are not detecting or reporting breach incidents at the same efficacy as postsecondary schools.

Based on our experience with small enterprises, we believe that that the later (#3) is the most plausible explanation. The large number of *unknown* profiles breached by K-12 schools also suggests that those schools could improve how their information assets are inventoried, managed and maintained.

State-operated postsecondary institutions, which report significantly more breach incidents, may be more attentive in reporting breaches because they are more keenly aware of state breach notification laws through their direct state affiliation and may be more cognizant of state and federal laws concerning identity theft, privacy and information security, compared to locally-operated K-12 schools. There should be cause for concern because of the increasing incidences of child identity theft.

Profiles Breached by Education Sector Category

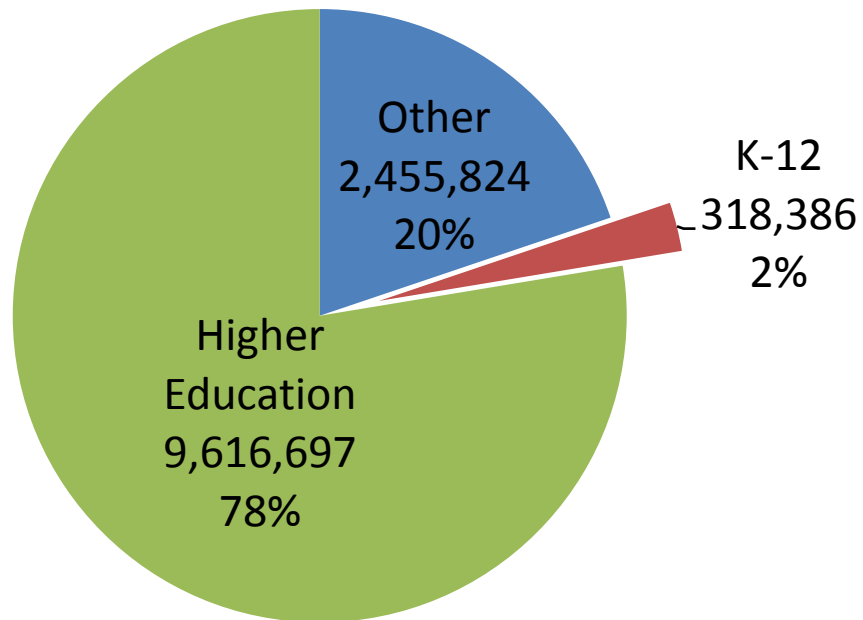


Figure 6. Profiles compromised by each of the three Education Sector Categories: K-12, Higher Education and Other (service providers and some regulatory agencies). Each of the three categories reported breach incidents where the estimated number of profiles compromised were characterized as unknown. K-12 characterized 30% of the breaches as affecting an unknown number of students and other consumers, followed by Other (14%) and Higher Education (9%).

In this study, we attempted to extract information regarding whose profiles the Education Sector was compromising. We did this by considering the descriptive content contained in both the description and the number of records compromised. After review of the 324 Education Sector breach incidents to examine how institutions were characterizing breaches, we categorized breached profiles as follows:

- Students (including alumni)
- Students and employees
- Employees including faculty, staff and employed students
- Unspecified (may include students)
- Other (includes parents and charitable donors)
- Patients & Study Subjects, which may include students

Because of the challenges we had with interpreting and categorizing incomplete descriptions of the information summarized in Figures 7 and 8, these results should be considered approximate.

The results show that in addition to student, alumni and employee profiles that a variety of other Education Sector patrons are likely to have their sensitive information compromised in a breach incident.

Figure 8 is a representation of this information that excludes all Patient & Study Subject Data (including the two largest Education Sector data breach incidents). Some may consider patient and subject data as Health Sector, although in our view the information was controlled by the Education Sector or at least by a hybrid sector consisting of Education and Health.

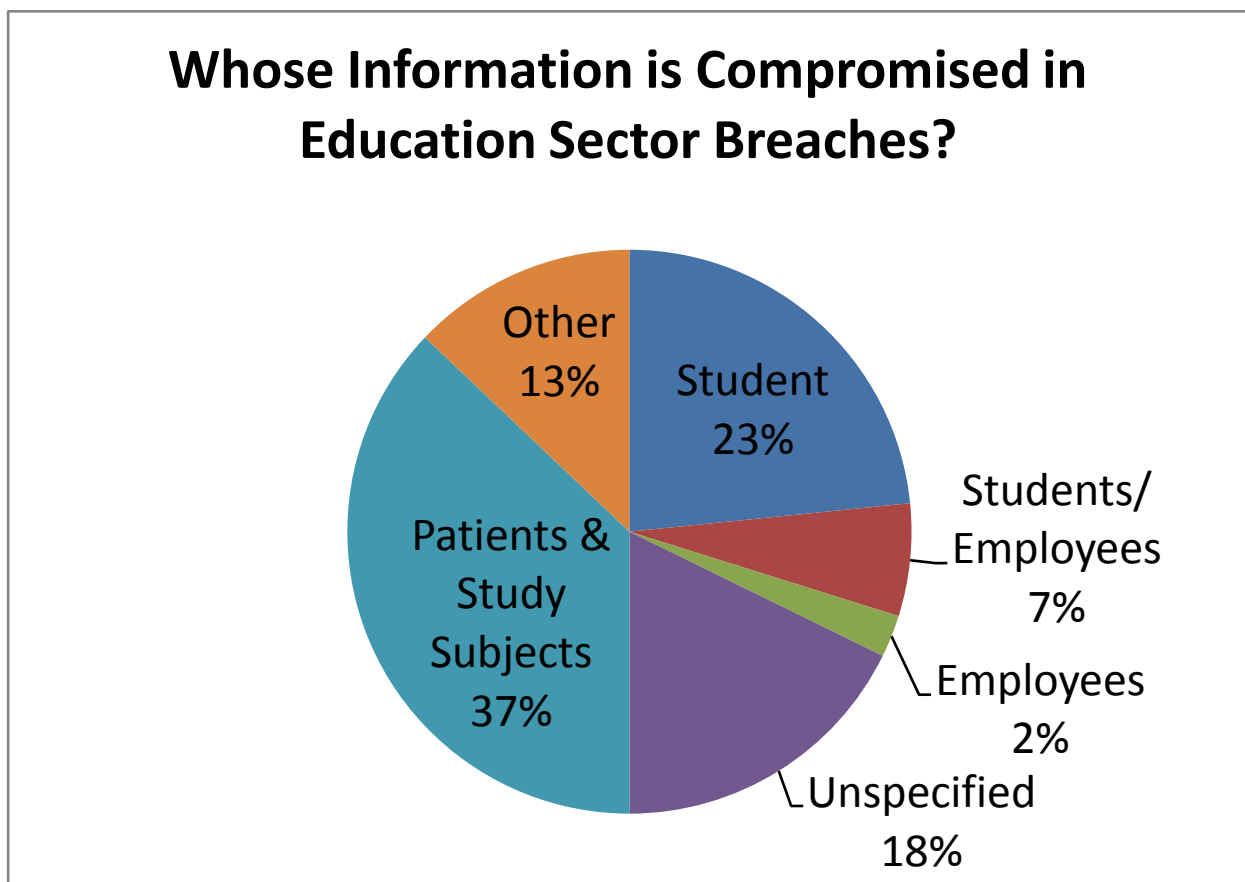


Figure 7. Breakdown of whose information is compromised in Education Sector data breach incidents.

Out of the 324 education-related data breach incidents, 24% were attributed to a hacker accessing information systems. However, there were many more breaches characterized as an “unauthorized person gained access to information” or a similar description, which raises the question as to whether the breach incident was simply an employee accessing information without authorization or whether it was a case of an outside intruder, a “hack attack.”

Over a third (35%) of the breach incidents were characterized as involving lost, stolen, missing, or improperly disposed computers, electronic storage devices, magnetic tapes, paper files and microfiche. Such breach incidents involving electronic storage devices accounted for 32%; “laptop-only” accounted for 15%; and traditional files (paper, microfiche) accounted for 3%.

Generally, we were not able to categorize the cause of about 40% of the breach incidents because of the disparity of the descriptions.

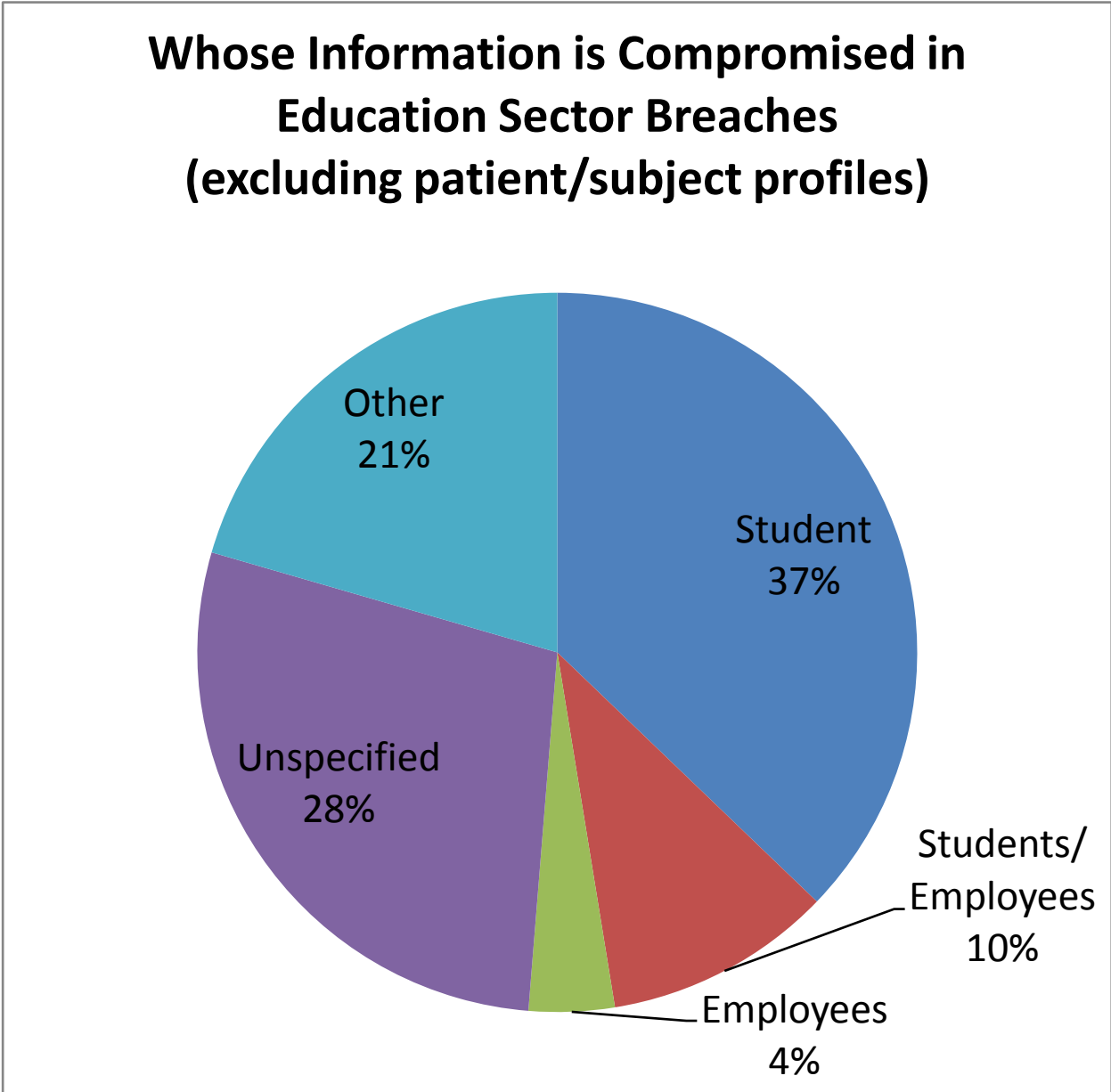


Figure 8. Breakdown of whose information is compromised in Education Sector data breach incidents after removing 4.6 million patient and study subject profiles from the comparison.

Conclusions and Recommendations

In this study, we described a range of scenarios that can be characterized as best and worse. Regardless of the scenario or rationale applied to interpreting the Education Sector breach incidents, the number of data breach incidents and profiles compromised by the Education Sector is disproportionately high compared to the total of all other U.S. enterprises that reported data breach incidents.

Table 1. Best and Worst Case Educational Sector Security Breach Statistics

Scenario	Education Sector as % of all Total U.S. Enterprises	Data Breach Incidents as % of Total Reported	Consumer Profiles Compromised as % of Total
Worst Case	0.6%	31%	5%
Best Case	13%	31%	25%

Breaches reported by K-12 institutions appear disproportionately low (15%) compared to those reported by the higher education category (79%) recognizing that there are more than 20 times the number of elementary and secondary schools compared to postsecondary institutions. This observation suggests that K-12 institutions may not be detecting or recognizing data breach incidents when they occur and may not be reporting data breach incidents even when they are recognized.

The large numbers of breaches (12.4 % of the total and 30% for K-12 institutions) that characterize the number of records compromised as *unknown* suggest that many schools do not keep an inventory of personally identifiable information that they maintain.

School staff and faculty should be able to recognize when information is potentially compromised when they have a rudimentary level of awareness training on identity theft, privacy and information security. While some breach detection can be accomplished through technology (especially computer hacking), a significant portion of breach incidences can be detected and prevented by increased awareness of faculty, staff and students.

Schools should begin investing in mandatory awareness education that includes all faculty, staff and, as appropriate, students. The program initiative must come from the top-level administrator: the superintendant, principal, president. Awareness education is relatively inexpensive yet, in our experience, education is the most effect strategy in getting all faculty and staff to safeguard sensitive information appropriately and to recognize risks and incidents that may lead to information compromise.

How would most faculty members answer the following question? If you lost a printed class roster containing student names and student identification numbers, what would you do?

- a. Nothing
- b. Request or print another copy of the roster
- c. Report the missing roster to the school privacy officer

This routine example, which represents a compromise of personally-identifiable information (a student ID Number), is covered under the Family Education Reform and Privacy Act (FERPA), likely goes unreported daily throughout U.S. schools. The majority of faculty and staff would not recognize such an incident as a data breach. Many institutions do not have a privacy officer to whom the data breach, in this case a missing roster, is to be officially reported.

Many Schools focus on FERPA, a privacy law that is limited with respect to current privacy and information security standards and best practices.

There are a number of other federal and state laws that potentially apply to educational institutions and a broader range of personally identifiable information including Social Security numbers, date of births, credit card and bank account numbers, addresses, telephone numbers, email addresses and health information.

Schools that have an infirmary or clinic may be considered hybrid entities under the Health Insurance Portability and Accountability Act, and would be required to protect student and employee health care information that they collect and transmit.

Schools that provide student financial aid may be subject to the Gramm Leach Bliley Act and the Fair and Accurate Credit Transactions Act Disposal Rule.

Many schools accept credit card payments for books, tuition, donations and other purchases. Schools that accept credit cards are subject to the Payment Card Industry Data Security Standard (PCI-DSS).

Most every state has a variety of identity theft, privacy and information security laws that apply to the public and private sector, the institution itself, the faculty and staff, and students. Faculty, staff and students should be aware of the civil and criminal consequences to the institution, as well as to them personally, if they mishandle personally identifiable information as part of their job responsibilities or if they commit identity theft or aid or abet someone in committing the crime.

Most every state has a breach notification law, and there is a federal notification law on the horizon. When a breach occurs, notification of the probable victims is mandatory.

In the absence of the laws referred to above, institutions as well as individual faculty and staff can held culpable under common law, should they be involved in the mishandling or negligent handling of student or other consumer personally identifiable information. For example, it is not uncommon to distribute sign-up sheets containing personally identifiable information in student classes, faculty training, professional seminars, and adult career development and continuing education. Some information on signup sheets may be considered "legally sensitive." In the wrong hands, such information can be used to invade privacy and for other more nefarious purposes such as harassment or identity theft. In a situation where a person on the list is victimized through the mishandling of the list, for example in a case of harassment, assault or identity theft, the faculty or staff member involved in collecting the information could face legal ramifications, such as being personally named in a law suit along with the institution.

Schools should invest in data encryption utility software. Contrary to common beliefs, data encryption is inexpensive, simple and easy to use. All personally identifiable information that schools and related service organizations maintain electronically should be encrypted. Data encryption would render electronic data accessed through hacking useless. Combined with identity management, data encryption can significantly decrease instances of unauthorized access by staff and students. Data encryption removes the risks associated with lost and stolen computers, electronic storage devices and magnetic tapes. Although encryption sounds intimidating, it should be embraced as a simple, inexpensive and effective approach to safeguarding sensitive electronic information.

Schools should contractually require all business associates (vendors, support organizations) with whom they share their constituent's personally identifiable information to maintain a privacy and information security best practices program and to comply with all applicable laws requiring the safeguarding of personally identifiable information.

Endnotes

¹ Stoops, N.; Educational Attainment in the United States: 2003, Current Population Reports, U.S. Census Bureau, Washington, D.C., June 2004.

² Privacy Rights Clearinghouse, San Diego, CA. www.privacyrights.org

³ Campana, J.E.; Privacy MakeOver: The Essential Guide to Best Practices, Bell House Press, Madison, WI (2008).

⁴ Statistics about Business Size from the U.S. Census Bureau (2004). Indicates that the total firms in the US is 25 million; Firms with employees account for approximately 6 million, and firms with 20 employees or more account for approximately 600,000.

⁵ U.S. Census Bureau 2002 Census of Governments. Of the 87,900 units of local government in the U.S., 13,500 were characterized as school district governments and included in our category of K-12.

⁶ National Center for Education Statistics, 2007 Digest of Educational Statistics.

⁷ National Center for Charitable Statistics, Number of Nonprofit Organizations in the U.S. 1996-2006. Of the 1.48 million reported, we included all Reporting Public Charities (347,000) and Private Operating Foundations (4,600) in the data illustrated in Figure 4.

This study was presented in part at the 2008 Association of School Business Officials International Annual Meeting, Denver, CO, November 2008.

About J. Campana & Associates and the Author

[J. Campana & Associates](#) is an identity theft, privacy and information security solutions consulting firm that specializes in compliance and risk management solutions for smaller enterprises. Dr. Campana is certified as an information privacy professional for both corporate and government operations and a certified identity theft risk management specialist. He is also the author of the book: [Privacy MakeOver: The Essential Guide to Best Practices](#). Dr. Campana is also a part-time faculty member at the Madison Area Technical College, Madison, WI, where he teaches insurance continuing education on identity theft, privacy and information security risk management.