

1

Campus Invasion: Security Breaches and Their Trends in Universities Across the U.S.

Christopher Cook & Morgan MacBaisey

Introduction

As a current or alumni university student, you may or may not know how much personal information the school has on file about you. You also may not realize how vulnerable this information is to theft and hacking. How would you feel if you received a letter or e-mail stating the following?

“A new case of unauthorized computer access has been identified at the University...The potentially exposed information includes about 49,000 database entries on a server containing ancillary information used by the Registrar's Office. The information dates from June 1999 to May 2001 and from fall 2003 to summer 2005...the University is notifying individuals of potential identity theft so they may take precautions. Sensitive information that may have been accessed includes: Social Security numbers, names, permanent addresses and phone numbers” (Boulder).

Every college student across the U.S. has the potential to receive a similar letter at any point in their college career and even after graduation. Krista, a student at the University of Colorado at Boulder, was studying abroad one semester when both she and her mother, a CU alumni, received letters containing the previous information. With her daughter abroad, Krista's mother thought nothing of it. Many months later, Krista received a letter from a credit card company notifying her of potential fraudulent activity present on her account. There was worse news to come: Krista did not even have an account with the credit card company that sent her the notification. The address they had on file for her was wrong. It was actually an address on the other side of the country where Krista had never resided. At the time she received the information from the credit card company, Krista had forgotten about the letter she had received from the University of Colorado. Krista ordered credit reports to verify the damage to her credit. She subsequently noticed that there was a correlation to when her school information was stolen and when the credit card account was fraudulently set up in her name.

An interview with the University of Colorado Records Department revealed that personal student information such as

telephone numbers, e-mail addresses, social security numbers (SSNs) and physical addresses are stored on file for an unlimited amount of time. Many schools also store their students' medical records. It was mentioned that no one could get this information without proper access. The truth is that this information is accessible. This being said, it is possible that you may receive a letter, like the one above, years after you graduate and have moved on with your life. One may think this information is harmless if obtained, but there is a potential for extensive identity theft as a result of a campus information security breach.

Data loss has occurred for centuries. To demonstrate the lack of privacy and security at universities and the severity thereof, consider the following incident. In the article "Social Security Numbers Exposed in CCSU Letters," "approximately 750 CCSU [Central Connecticut State University] students have received mail from the Bursar's office that revealed their SSN's in the name and address window of the envelopes" (Attrition). Surprisingly, this egregious mistake occurred on February 7, 2007. It would seem as though Universities would be more careful in protecting their databases in 2007, considering the growing prevalence of identity theft over the preceding years. This chapter will examine trends with regards to university information privacy across the U.S., student opinions and knowledge of data theft and information privacy, as well as a discussion of worst-case scenarios, and the role of the media.

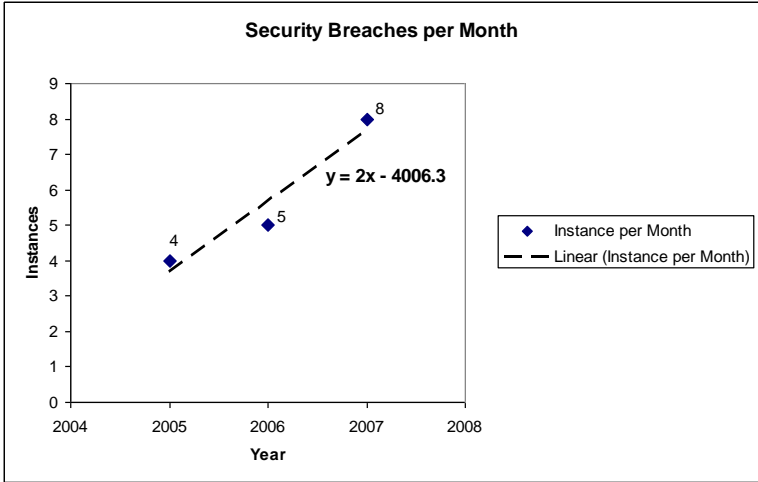
Trends Across the Country

Out of the hundreds of universities in the U.S., a recorded 177 schools have had one or more instances of security breaches in the last two and half years. Information about students, faculty and alumni was illegally stolen or accidentally released. This information included everything from a person's social security number (SSN) to their semester class schedule. As an increasing number of universities with security breaches were discovered, trends began to emerge in terms of public versus private universities, the location of the schools themselves and the methods of the breaches.

A complete chronology of data breaches of universities across the country has been documented on the Privacy Rights Clearinghouse (PRC) website. The PRC details each breach by when it happened, the number of people affected, and exactly how the information was stolen. We used the information from the PRC to examine the different trends with regards to security breaches. Our analysis used a simple random sample of 50 schools from 2005 through March 2007. The average number of people affected by each breach was 41,780. Some schools did not release the number of people affected or simply stated "tens of thousands" of people. As an example, the University of Southern California, ranked number one, with 320,000 people put at risk. At times, the number of affected individuals from any single breach can be much larger than the current student body. This is because the number of individuals affected includes past students, faculty, alumni, and even prospective students who have applied to the University.

One of the first trends found was the number of schools breached over the past two and a half years. Our research clearly indicates an increase in the total number of schools experiencing security breaches yearly. This increase is attributed to the constant

advances in technology, as well as the increasing volume of personal information stored on line and web accessible files (such as online databases). Historically, a select few possessed the skills and knowledge to successfully hack and steal information. However, in recent years, the necessary skills have become more prevalent, and the essential technologies became widely available. Through the analysis and collection of secondary data, the graph below demonstrates the trend of security breaches per month.



As you can see from the equation of the trend line, every year the rate is increasing by two breaches per month. From this information, we can estimate that in 10 years, the monthly security breach rate will increase to 28 separate instances of information loss per month from schools across the country. That translates into millions of people's private/personal information in the hands of the wrong people.

Hacking

People find interesting ways of getting a hold of people's information stored on university property and databases. This ranges from simply stealing a professor's laptop to actually creating programs to hack into a schools' computer system. Either way, information is being stolen and made available for a variety of negative uses, which can lead to identity theft.

Also analyzed for trends was the culprit, or who was stealing the private information. Out of the sample of 50 schools, the statistics on how the information was lost as well as who actually committed the crime is listed below.

Method of Breach

Percent of Schools Affected by Hacking	84%
Percent of School Affected by Internal Errors	16%

Culprit

Number of Schools Affected by Insiders	20%
Number of Schools Affected by Outsiders	54%
Unknown	26%

Of the 50 schools, 84% fell victim to hacking. It is important to note that this method of breach includes, but is not limited to physical computer theft. This is not surprising due to the ease and anonymity of hacking. Looking at the culprit statistics from the sample, 54% and 20% of schools were affected by outsiders and insiders respectively. In June 2006, at the University of Texas in El Paso, "students demonstrated that the student body and faculty elections could be rigged by hacking into student information (databases) including SSN's" (Data Breaches). This illustrates the ease at which people can gain access to private information. There is significant motivation for individuals to want access to information stored on university databases. This motivation ranges from money gained through stolen identities, to popularity and power achieved by rigging elections. At the University of Texas in El Paso, 4,719 students and university personnel were put at risk for identity theft from this simple demonstration.

In another example, at the University of Colorado at Boulder, "two computers had been placed in storage during the school's move to temporary quarters in May. When they were to be retrieved August 28, they were found missing. They had been used by two faculty members and included students' names, SSNs, and grades" (Data Breaches). It does not take knowledge of computers to steal information. It is a matter of being in the right place at the right time.

There have also been occurrences of schools accidentally posting confidential student information on their website. This recently happened in March 2007 at the University of Idaho where "a data file posted to the school's Web site contained personal information including names, birthdates and SSN's of University employees" (Data Breaches). Because of the school's error, 2,700 people were put at risk for identity theft. Another recent mistake occurred at the Los Rios

Community College in Northern California where “student information, including SSN’s, were accessible on the Internet after the school used actual data to test a new online application process in October” (Data Breaches). At least 2,000 individuals were put at risk.

Not only are hackers getting access to people’s SSN’s, but in some cases they are gaining access to credit card information as well. At East Carolina University, “a programming error resulted in personal information of 65,000 individuals being exposed on the University’s Web site. The data has since been removed. Included were names, addresses, SSNs, and in some cases credit card numbers” (Data Breaches). Incidents like this put university members, many times unknowingly, one step closer to having their identity stolen. Our research indicates that personal information is at risk from not only outsiders, but also the threat lies within the university itself where many would not expect.

Public versus Private

It was found that 64% of the schools breached were public Universities. We hypothesize that this is due to the greater number of students (student body and staff) at public schools. In other words, hackers have a greater pool from which to potentially steal valuable information. Private schools experienced a lesser percentage of breaches, but this does not mean the loss of information was any less detrimental to the affected individuals.

An alternative hypothesis for this result is that private schools may not be subject to the same requirements and standards as public universities. This may lead to skewed statistics. The truth may be that private schools do in fact have a higher percentage of breaches, but they are not required to make the instance public, containing the knowledge of the breach. This is exactly the problem that needs to be addressed in public and student policy.

East Versus West

It was interesting to see that more West Coast schools were experiencing instances of information breaches. Analysis indicated that 64% of our sample was located on the West Coast—leaving only 36% of instances on the East Coast. (Note: we divided the country in half and did not include a third category for the central U.S.) When students are faced with the decision of which side of the country to attend college, many factors are taken into consideration. These may range from climate difference to the distance from home. According to our research, students may want to ask themselves one last question: “Am I willing to take on greater risk of information loss by attending a West Coast school?”

Student Survey Information

By analyzing the frequency, location, and trends of security breaches across the U.S., it is apparent that data theft is rampant. Not many students have the luxury of knowing their information is actually at risk before their information is stolen. Unfortunately, students must be aware of the risk in advance to be able to take the necessary precautions for protection. It takes awareness and motivation on the part of the individual alone because in many cases, no one is going to explicitly tell someone that their information is at risk.

According to the Identity Theft Resource Center (ITRC), "college students are easy targets for identity thieves because it takes the average student longer to discover the fraud. In a recent report, almost 90% of student victims were unaware of their compromised identity for several months" (CU Identity Theft). Having access to students across the country through family, friends and online social networks, a survey of past and current university students was conducted to examine the awareness and knowledge with regards to various topics related to information safety and privacy at universities.

The survey was created using surveymonkey.com, an online data analysis company. This company allows users to create a free ten-question survey and provides the user a web link for the pseudo webpage containing the survey. This hyperlink can be sent to any individual with access to the Internet. By clicking on the link, respondents are redirected to the requested survey. Our survey contained ten questions, ranging from "yes or no" questions to individual "short-answer" responses. 75 surveys were returned by individuals for our analysis. The survey was sent to a random sample of individuals across the U.S. and allowed for generalizations to be made that encompass students attending private, public, and East / West Coast schools. This is an important aspect of the analysis because bias and area specifics wanted to be minimized. Below are a few examples of our most telling survey questions and their corresponding statistics. (Note: all surveys were anonymous.)

First, respondents were asked whether they were currently attending a university followed by how many years they have been enrolled. Out of the 75 respondents, 80% are currently enrolled in school. There are 48.6% in their fourth year, 15% had been enrolled for less than one and 15.4% had been students for more than four years.

The next question asked if they had been aware of any security breaches where their private information could have been compromised. Surprisingly, only 37% said yes. They were then presented with this question:

"Have you ever received a letter/e-mail containing information similar to the following: A new case of unauthorized computer access has been identified at Your School. The potentially exposed information includes about 49,000 database entries on a server containing ancillary information used by the Registrar's Office. The new incident creates a potential identity theft problem for former students and some current students. Sensitive information that may have been accessed includes social security numbers, names, permanent addresses and phone numbers."

Of the respondents, 37% (as above) said that they had received a similar notification. Interestingly, 15.1% responded, "maybe, I do not

remember.” Out of 75 people 12 do not even remember if their information was potentially stolen. Recall, from the section above, the average university population affected by each security breach is 41,780. Now realize that that equals a potential 6,267 individuals who do not remember if their information was compromised. This number is daunting when put into context of total security breaches per month.

Our survey indicates that 88.1% of students that received the notification did not take any of the suggested precautions detailed in the letter. Precautions include contacting the three major credit bureaus (Equifax, Transunion, and Experian) and putting an identity theft fraud alert on your file. A fraud alert stops new offers of credit to be extended for up to seven years and increases awareness on your account. However, “this is an advisory statement and has been found to be only partially effective” (Reporting). A more comprehensive and effective recourse is to get a “credit freeze in states that have passed that legislation” (Reporting). A credit freeze requires authentication from the individual to make any modification, however small, to the account. There are precautions and steps for individuals to take to limit their risk. However, many college students have a very trusting and naive attitude when it comes to the security of their private information stored with universities.

Respondents were asked to indicate which of the following personal information they think their school has on file about them. The following list was presented: social security number, telephone numbers, gender, permanent address, local address, medical records, marital status, information about your family, financial information. 98.6% said they know the school has their social security number, telephone number, gender, and permanent address on file. Only 56.2% of our respondents knew that the schools have their medical records on file. 83.6% said they had financial information, 76.7% said they had information about their family on file. Schools actually have information on students ranging from address, social security number, medical history, and in case of students that use financial aid, your financial information.

Individuals were then asked to rate on a scale of one to five, how at risk they felt their personal/private information was at their university with five being extremely vulnerable. Of the respondents, 63% answered between zero and two, indicating they felt their information was either not at risk or low risk. Furthermore, 45.2% of respondents felt that it was solely the universities’ responsibility to protect their private information held by the school. Students need to realize that they no longer can put the security of their personal identity in the hand of some of the most accredited institutions in the country. Even though there is no realistic way that a student can protect information held by the university, they must realize that constant vigil must be taken to make sure that if their information is compromised, they are aware and can take remedial action. This includes checking your credit report. 54.8% of respondents said it was the responsibility of both the individual and the university to protect their information. This idea is more realistic.

The last question asked of the respondents was how they would feel if their personal information were stolen from their university by a hacker. The responses to this question varied. One individual said “I guess I wouldn’t be surprised. The student database has been hacked

before and it will probably get hacked again. If I knew my information had been accessed, I would review my credit reports and update as many of my credit accounts as possible.” This individual was one of the respondents that have received one of the security alert letters in the past, but who have also read what to do in case of a breach. It is alarming that he/she said they would “not be surprised.” Today, the majority of students are desensitized to the severity and importance of their private information. By the time they have filled out their college applications students may have potentially printed their social security number on over 20 pieces of paper. One respondent said they would be “shocked,” but that there was “realistically probably nothing [he/she] could do. [And] unfortunately those things happen.” There are steps these students can take to prevent and protect themselves. As our research indicates, many students are either unaware of their options or have come to accept the fact that their information will be stolen. This is the wrong attitude to move into the 21st century.

Humans tend to be oblivious, or ignore the severity of any situation unless they are obviously negatively impacted. Having your information lost by the school is a direct negative impact, but as our research shows, this is not enough of a threat for many students to feel at risk. In turn, appropriate action is not taken. Until actual identity theft and financial damage occurs to more students from these security breaches, it is unlikely that we will see a change in attitude. One respondent proved this exact point. They said they would feel “frightened” if their information was stolen and that they would “have to go through and cancel credit cards and would constantly be afraid, and on the look out for identity theft in the future.” Students need to be “on the lookout” for identity theft now and prevention is the only real protection.

Worst Case Scenarios

With peoples’ information at risk on campuses across the country, there are many examples of worst-case scenarios where identities have been stolen. These people can not directly prove their identity was stolen due to the hacked information at their school, but there was an interesting correlation in the timing of events in all cases.

As previously mentioned, at the beginning of this chapter, Krista had her identity stolen right after her private information stored on university computers was stolen by a hacker. Her credit scores are now lower and she has had to place a security alert on all of her accounts. Krista lives in fear of future financial damage and identity theft due to a single security breach at her university.

In a similar case at the University of California at Los Angeles (UCLA), the school discovered that someone had been hacking into their schools databases for an unspecified amount of time and about 40,000 people were at risk. Although the school downplayed the threat and told potential victims that “there was no indication the information had been misused,” one student at UCLA also had their identity stolen (Breach Effect 1). He said, “I can’t prove my identity was stolen from this UCLA break-in, but it certainly is quite a coincidence” (Breach Effect 1).

Schools Starting to Take Notice

Due to some of these “coincidences” schools are finally realizing they have to be more vigilant in protecting student information. Many schools are no longer using SSN’s as student identification numbers and, in one case at California State Fullerton, the school no longer “keeps alumni information in its student database” (Breach Effect 1).

A recent policy was adopted by the University of Minnesota after three different incidences of breaches took place. It states, “the University shall provide timely and appropriate notice to affected individuals when there has been a breach of security of private data about them” (Reporting). It goes on to define what exactly they mean by a breach in security, “a breach in security occurs when there is an unauthorized acquisition of private information maintained in any form by the University” (Reporting). This simple regulation, however minimal, allows the plaintiff to at least be notified of the breach so they can take remedial action. Before this regulation, it was not explicitly stated that a university must inform affected students of breaches. This, for now, is the best the school system has to offer. Unfortunately, it offers little in terms of protection; the focus right now is prevention and the minimization of damages.

Media’s Role

When thinking about breaches in university’s security and information loss, one probably does not think about how the media plays a role. The media brings light of the situation to the public, beyond just the university students. “The media frenzy surrounding each security breach has helped put consumers and merchants alike on the alert; once notified, many victims quickly get on the horn with their bank and credit-card company” (ID Theft 35). The media’s role has increased over time and helps to raise awareness about the importance and volatility of private information. As seen from the survey, most students do not even realize how serious these incidents are and so the media is playing its part in prevention. By publishing or broadcasting articles and stories about breaches, the media helps to bring knowledge and awareness to students.

Conclusion

Every year, thousands of students send applications to colleges across America and trustingly place their private information in the seemingly secure hands of universities. These applications and student files contain personal information, such as SSN’s and credit card information, that if obtained by the wrong people could have a devastating affect on their lives. Our research was conducted in attempts to gain knowledge and identify trends across the country with regards to university student information privacy. By conducting surveys of students and faculty, as well as studies on actual university information security breaches, it has become apparent that there are indeed countrywide trends regarding information security. It was found that West Coast schools and public institutions have a higher percentage of security breaches than East Coast and private schools. The

frequency of breaches is increasing at a daunting rate of two schools per month, and the average breach affects 41,780 individuals.

Many universities are lackadaisical and relatively passive with their approaches to information security. A majority of students feel their information is safe in the hands of their university when in reality it is at risk. Many students do not feel or are unaware that there are steps they can take to reduce their risk of possible identity theft if their information is, in fact, stolen. These misconceptions must be corrected. Universities need to work with the students to find ways to better ensure the safety of personal information they store on file. With advancement in technology and the skills of hackers greatly increasing, universities need to minimize avoidable internal errors that put students at an unnecessary risk. As mentioned before, it needs to be a collaborative effort. Students need to heed the breach notifications that schools send out, as well as take the preventative measures outlined. Unfortunately this is an evolving and growing problem where complete protection is not possible. Minimizing risk is the only alternative.

Works Cited

- Attrition. 2007. Feb 14, 2007. <<http://attrition.org>>.
- Boulder. 2007. University of Colorado. 14 February, 2007. <<http://www.colorado.edu>>.
- CU Identity Theft. 2007. University of Colorado at Boulder. 13 March 2007. <<http://www.colorado.edu/its/security/awareness/privacy/>>.
- Data Breaches. 2007. Privacy Rights Clearing House. March 2007. <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>.
- Foust, Dean and Ryst, Sonja. 2007. ID Theft: More Hype than Harm. Business Week; July 2006 Issue 3991, p34-36. <<http://businesssourcepremier.com>>.
- IDRC. 2007. Identity Theft Recourse Center. 13 March 2007. <<http://www.idtheftcenter.org/vg100.shtml>>.
- Reporting and Notifying Individuals of Security Breaches. 2007. Reporting. 13 March 2007. <http://process.umn.edu/groups/ppd/documents/policy/securitybreach_pol.cfm#100>.
- Wolfe, Daniel. Breach Effect. 2007. American Banker. January 2007, Vol. 172 Issue 9. <<http://businesssourcepremier.com>>.