



Breaches in the Academia Sector

by
John Correlli, Esq., CIPP

In trying to make sense of the sheer volume of privacy data breach incidents occurring in the academia sector over the last 3 years, there has emerged the ‘top three’ most common breaches occurring at universities and colleges throughout the united states. Those breaches have affected schools all across the country, with certain states suffering significantly more than others.

A.

Top 3 Reasons for Privacy Data Breaches in Academia

1. Topping the list are incidents occurring as a result of unauthorized access to computerized privacy data. What is important to note is that the *unauthorized* part is often accomplished *not* by strangers (some cyber criminal sitting in a dark room half a world away), but from inside individuals - employees, students, third party vendors, etc. who don't have permission to access digital personal identity information (PII) at their organization.
2. Next are data breaches resulting from accidental online exposure of privacy data - whether from being inadvertently posted directly to a website page with readily available viewing, or to a web file that may also be readily accessed as a result of some other online activity.
3. The third most common type of incidents are privacy breaches resulting from stolen laptops - stolen in the sense that either the laptop itself was wrongfully taken, or the laptop was in a vehicle that was stolen.

From 2005 through 2007, there were approximately 277 breaches occurring at universities and colleges, and of those:

- 89 were a result of some type of unauthorized access;
- 45 stemmed from accidental online exposure; and
- 37 resulted from a laptop computer being stolen.

Why are these 3 types of breaches the most common?

I. Unauthorized Access

Unauthorized Access is first for a number of factors:

1. *Universities and their computer networks are typically open environments.* Though they may come in various shapes and sizes, most institutions promote the open exchange of ideas, often requiring an open environment both physically (i.e. no doors, or doors

that remain open, many windows, etc.), and electronically, in which databases are shared inter-departmentally. Although universities are becoming more aware of the risk to computerized privacy data, there still exists an electronic 'blind-spot' to those risks. That 'blind-spot' is then exacerbated by the 'open-environment' approach.

2. *Opportunity for wrongful access.* The sheer volume of computerized information regularly acquired and maintained by an institution, along with the ease in which that data can be wrongfully accessed, provides a climate ripe for breach incidents.

3. *Breach disclosure laws.* This computer-age phenomena has resulted in Breach Disclosure Laws being enacted by most states over the last five years. Generally speaking, the law requires that any wrongful access of ***unencrypted computerized PII*** mandates that the incident be publicized. It's a domino theory:

- More computerized information leads to more wrongful access incidents.
- More wrongful access incidents leads to more breach incidents.
- More breach incidents leads to more notifications, which leads to more publicity.
- The more a certain type of data breach is publicized, the more common it appears.

4. *Human error.* Quite often, human error and technical problems lead to unauthorized intrusions. Data breaches can originate from many places (unlocked file cabinets/office doors; a server's security settings being improperly configured) - leaving sensitive data not fully protected.

5. *Unrealistic dependence on IT security.* In trying to avoid wrongful access, institutions sometimes assume that just by purchasing security software/hardware before or after an incident, all future breaches will be prevented. They 'check off the box', by buying a 'cure-all', instead of diving into the data breach risk problem and implementing a 'best practices' prevention program organically (from the inside out). Sometimes the delivery of IT security software actually results in the overall system to be less secure.

6. *Home grown help.* As in other sectors, universities and colleges will sometimes utilize in-house personnel to address existing and future data breach risks, rather than engaging outside experts. Obviously a product of cost-benefit analysis, the institution's own IT people (or other security or risk-management staffers), may not always be up to speed on the latest security risks, be it an iteration of a previous access attempt, a new method of PSES (persuasive social engineering skills), or other common but pervasive privacy data risks - i.e. careless storage and disposal practices.

7. *The use of social security numbers.* Although more institutions are converting to school-issued ID numbers, removing social security numbers from all universities' business practices can be an enormous, expensive, and time/personnel consuming process. As such, remaining social security numbers (and a huge number still exist), offer an inviting target to identity thieves.

CAVEAT: Although unauthorized access still leads the list, the rate of incidents has decreased - from 45 in 2005 to 21 in 2007, most likely as a result of social security numbers being utilized less and less as identifiers.

8. *Whistling past the graveyard*. How often is it heard at the end of a report about a publicized data breach:

‘A university official said . . . *there's no evidence* that any unauthorized individuals have actually retrieved or used any personal data on the computer’

or

‘. . . the institution *is not aware* of any identity theft cases stemming from the computer break-in’

or

‘. . . the university *suspects nothing* will come of it’.

Just fill in the blanks . . .

A common attitude among organizations that publicly discuss the likelihood of consequences resulting from a breach incident is that: if there have not *yet* been any identity thefts, or other ramifications discovered as a result of the breach, then there *won't be* any consequences.

But, what many of the decision-makers don't grasp, (at least externally), is that stolen privacy data is like fine wine - it becomes more valuable with age. And it does not need to be used immediately. An identity thief can sit on PII for months, or years, then use it or sell it after the victim's initial privacy concerns have subsided, and/or their safeguards have lapsed (i.e. 90-day fraud alerts; credit monitoring subscription expires).

- In April, 2005 Florida International University suffered a data breach and publicly acknowledged the incident. The FIU spokesperson stated: “*There's no evidence that any fraud has taken place as yet. . . . Technicians will be updating operating system and anti-virus protection, removing known vulnerabilities, re-configuring log-in accounts, scanning for applications that allow for unauthorized access as well as disseminating new information on effective password management and computer user access guidelines . . .*”.

Yet, less than a year later, in May 2006, FIU publicized another breach as a result of a **computer infected with malicious software allowing unauthorized access** to students' social security numbers.

- And as recently as July, 2008, as reported in [The Dallas Morning News](#), the University of Texas at Dallas suffered a computer network attack which may have exposed social security numbers and other privacy data of over 9,000 individuals. The compromise may be attributed to a security breach in the university's computer network, but a school spokesman said that they had found “*no indication that the information has been disclosed, disseminated or used to anyone's detriment.*”
- The newspaper also reported that the *same university* had also been hacked in 2006, in which the privacy data of 35,000 faculty, staff, students and others was possibly compromised.

As a direct consequence of an open environment, lack of comprehensive risk assessment oversight, out-dated use of social security numbers as identifiers, and slow, and/or non-effective reaction to the latest data security risks, unauthorized access rests atop the list of privacy data breaches in the academia sector.

II. Accidental Online Exposure

For the most part, 'accidental' provides the definition in the term, as to why this type of breach occurs so often, and unsurprisingly, is the second most common among academia.

1. *Negligence.* Though there may be varying degrees - *carelessness, laxity, inadvertence*, all accurately describe why, so often, privacy data is exposed online.

- In April 2006, Purdue University disclosed that personal information was **inadvertently** stored on a university business services computing Web site.

Less than a year later in March, 2007 Purdue then disclosed that students' personal information had been posted on a web page **inadvertently**.

- The University of Kentucky in May, 2006, disclosed that the institution **inadvertently** posted about 1,300 employee social security numbers on a public Web site.

Three months later in August, 2006, Kentucky then disclosed that the social security numbers of students were **accidentally** released publicly in *two* separate incidents. . . . which brought to *four* the number of times that year in which personal identity information was **accidentally** released at the university.

2. *Processes.* Sometimes, even when an organization is correcting one problem, it causes another.

- The University of Nebraska - Lincoln disclosed that in March, 2006, social security numbers were accidentally posted online because the web site that caused the problem was created **before** the university began **converting** to university-issued student ID numbers.
- In December, 2005 the University of Dayton disclosed a **programming error** which exposed online social security numbers and other privacy data of applicants to the university's pre-med program.

3. *Oversight.* (Lack thereof)

- City College of New York disclosed in September, 2005, that an **unprotected payroll link** exposed privacy and payroll data online.

- In October, 2007, the New England School of Law disclosed that privacy data belonging to school alumni was **available** on a page of the school's website through Google.

And a recent example occurred in July, 2008, at Ohio University, where privacy data of almost 500 speakers, (many of them doctors and nurses who give talks to residents as part of their medical training), was posted online as a result of a clerical error.

Carelessness has many names. When coupled with so many opportunities in the academia sector to display PII online, its no 'accident' that this type of breach (*online exposure*) ranks second among privacy data breaches.

III. Stolen Laptops

A laptop being stolen is not unforeseeable. It may not even be preventable sometimes. But, the following are reasons why stolen laptops turn into public relations nightmares for universities, colleges and other organizations, and why these rank as the third most common type of privacy data breaches in academia:

1. Absence of written laptop security policies: A common oversight in the academia sector is the lack of specific written policies recognizing and addressing the privacy data risks inherent in the use of laptops.

- In July, 2006, The University of Iowa disclosed that a laptop containing privacy data of 280 current and former students was stolen from a professor's office. The university was in the process of converting social security numbers with student ID numbers, but the process had not been completed by the time of the breach. A spokesperson said the university ***did not have a policy*** about storing PII on laptops and other mobile devices.

2. Unnecessary storage of privacy data. A laptop's convenience is also its biggest privacy data weakness. Users sometimes will use a laptop as if it were a flash drive - storing information that may or may not be needed in the future, but is being stored simply for convenience's sake.

- In September, 2008 the Pittsburgh Post-Gazette reported that graduates at the University of Pittsburgh College of Business Administration were notified that a laptop containing their PII had been stolen. The laptop was being used by a university employee to survey alumni. A spokesman for the university said that "although the use of the laptop for the survey was proper, the storing of social security numbers on the laptop **violated university policy,**"

3. *Information used for the wrong reasons.* Coupled with reason number two is the third reason: The information stored in laptops is used for the wrong reasons:

- In March, 2006, Metro State College in Colorado suffered a privacy data breach when one of the school's laptop computers containing privacy information on more than 93,000 students was stolen. A college employee had been using students' PII *to write a grant proposal*, as well as *a master's degree thesis*. The problem was compounded by the fact that the institution was still using social security numbers as identifiers, instead of school-issued ID numbers.

4. *Unencrypted electronic data.* Common among many state breach disclosure laws, any computerized PII that is encrypted provides a clear *exemption* to disclosure. Unfortunately, laptop encryption is still not used on a wide-scale basis in academia and businesses today.

5. *Mobility.* Although it may seem that a laptop's mobility would be the number one reason why they are often stolen - which then leads to privacy data breaches - it's not the actual *taking* of the laptop that is significant, instead it's the content contained therein. If the stolen information is not privacy data, or if the privacy data is encrypted, the inherent mobility of the laptop would have no bearing on the number of breach incidents that occur and are publicized.

6. *Laptops and cars.* From 2005 through 2007, approximately twenty-five percent of all laptops stolen were taken from vehicles. This may not be the most significant reason for these types of breaches, but the tragedy is that these particular types of incidents are clearly avoidable. If not yet included in all university best practice policies, the prohibition of laptops left in unattended vehicles should be mandatory, along with penalties for violating the policies.

7. *Password protection is no protection.* When a breach is publicized, a university spokesman may often say that 'despite the theft, the privacy data on the laptop was *password protected*'. This misguided false sense of security provides another reason why stolen laptops reside so high on the list of academia privacy breaches. As the Identity Theft Resource Center (located in San Diego, CA) indicates when reporting publicized breaches - "a password is not adequate protection for computerized privacy data". Deciphering one-factor authentication is well within the capabilities of many identity thieves these days.

8. *3rd party vendor security policies.* Third party vendors will often utilize laptops when providing services to academia. When those laptops acquire PII, the vendor should be required to have data privacy policies in place, and reviewed by the university *before* any PII is transferred. Even if the vendor is at fault for the loss of the laptop, the institution will also be required to disclose the breach to all potential victims.

Lack of review of vendor security policies, along with the other reasons cited above, all contribute in helping *stolen laptops* to be ranked as the third most common type of privacy data breaches and put academia reluctantly in the news.

*** Additional Significantly Contributing Factors**

Apart from the different ways discussed above which lead to privacy data breaches, there are other equally significant contributing factors, including, but not limited to:

1. ***Lack of Privacy Data Assessments.*** Undergoing comprehensive privacy data risk assessments (physical/visual as well as digital) is *still* the exception rather than the norm in the academia sector.
2. ***Resisting Change.*** Some academia department heads have been in charge of a particular department for a long period (sometimes decades), and those individuals may not be as amenable to change as others when it comes to recognizing and addressing the privacy data risks and challenges facing academia today.
3. ***Fiefdoms.*** Along with resisting change, different university departments are sometimes akin to fiefdoms, where policies and procedures issued in one department do not necessarily apply in another. Just as different state laws may conflict in the absence of a superseding federal law, the same sometimes applies in academia - without one overarching policy, different university departments may have varying, or conflicting, or even non-existing data privacy policies.
4. ***Transitory nature.*** The transitory nature of individuals (students) involved in academia, combined with the volume of student (and sometimes personnel) turnover makes it difficult to maintain both consistent and current best practices in data privacy protection. Each semester brings new students with more and more privacy data to be accessed.
5. ***Number of Publicized Breaches Deceiving.*** Keep in mind, the breaches discussed above are only those that were publicized in compliance with applicable state breach disclosure laws. There likely were many more breaches which universities and colleges experienced, but weren't required by law to disclose; or perhaps chose not to disclose; or may not have even been aware of.

Of the 263 reported privacy data breaches in the U.S. in 2008, 76 (nearly one-third) occurred at universities and colleges, (and that's not counting breaches that occurred at the elementary through high school levels).

And a number of universities in the past 3 years experienced more than one type of breach - e.g. a school may have been 'hacked' and suffered 'accidental online exposure' in two separate incidents, such as what happened to Northwestern University, when in March, 2005, it suffered a breach caused by a 'hacker', then in June, 2007, another breach occurred when privacy data was accidentally posted online.

B.
Why the Top States Have Suffered the Most Privacy Data Breaches.

Although reasons may vary as to why some states rank higher than others in the occurrence of privacy data breaches in the academia sector, certain factors, in combination, appear to provide the most likely basis for the answer:

Population

- In the latest state census, California ranks first in population with over 36 million people. In the 2005 - 2007 survey of privacy data breaches in academia, California, (no surprise) also ranked first with 46 incidents (17 % of all publicized breaches) during that period.
- Ohio, which ranks 7th in population overall with 11.5 million people, suffered the second most breach incidents with 21 (8% of all publicized breaches).
- Texas and Georgia rank 3rd and 4th respectively in publicized breach incidents. Texas is the second most populous state with 24 million people and Georgia is also in the top 10 with 9.5 million.

With the rate of breach incidents being commensurate with population, size of population appears to be a contributing factor of breach occurrences among the states.

Enactment of Breach Disclosure Laws.

The emergence of breach disclosure laws (BDL's) among the states also corresponds with the ranking of states most affected by academia breaches:

California (ranked #1) - The state that began it all - enacted the country's first breach disclosure law in 2003. Texas, ranked third, enacted their BDL in 2005, along with nine other states. Ohio, which is ranked second, enacted their BDL in 2006.

Other states may have enacted their BDL's sooner than Georgia (which is ranked fourth and only enacted its BDL in 2007). But, coupled with the size of its population (9th), it makes sense that, the larger the population affected by the law, the more incidents would occur, and therefore the more incidents would have to be reported - pushing that state higher on the list, and in Georgia's case, to number four in publicized data breach incidents.

Only Michigan, which also enacted their BDL in 2007, has more people, (500,000), but ranks lower than Georgia, at number eight in reported breaches.

Number of universities and colleges.

- California has over 130 institutions of higher learning (second most in the country), and ranks first among reported breaches.
- Ohio, ranked second in reported incidents, has over 70.
- Texas, ranked 3rd, has over 100 colleges and universities.
- Georgia, ranked 4th, has over 50, which by itself, is almost double the number of institutions that exist in most other states.

Other Factors

There may be other factors at work in influencing which of the states suffer more academia breaches than others, such as:

- specific targeting of certain geographic areas by identity theft crime rings; and
- the timing of funding allocated to particular institutions or departments within institutions located in certain states.

As such, the confluence of population size, number of learning institutions, and the timing of breach disclosure law enactment, has resulted in California, Ohio, Texas and Georgia ranking first through fourth as the states most affected by publicized privacy data breach incidents.

Conclusion

Because of size, population and a generally 'open' environment, academia will remain a fertile ground for privacy data breaches. Sincere awareness and a proactive approach in addressing risk, along with effectively implementing best practices, can reduce the likelihood of data breaches at universities and colleges. Doing so will help both the individual and the surrounding community in the constant struggle to protect privacy information.



© 2009 Copyright

John Correlli, Esq., CIPP

JMC Privacy Consulting Group

Privacy Data Protection in the Workplace

3835 R E. Thousand Oaks Boulevard

Suite 119

805-230-2545

INFO@JMCConsultingGroup.com