

# **Educational Security Incidents (ESI) Year in Review – 2006**

**Author: Adam Dodge**

Copyright © 2007 Adam Dodge unless otherwise noted  
All rights reserved

# Table of Contents

<b>PART 1: INTRODUCTION</b> .....	<b>1</b>
BACKGROUND .....	1
DEFINITIONS.....	2
SOURCES .....	3
<b>PART 2: FACTS AND FIGURES</b> .....	<b>4</b>
INCIDENTS BY TYPE OF INCIDENT.....	5
<i>Incident Type - Theft</i> .....	6
<i>Incident Type - Impersonation</i> .....	7
<i>Incident Type - Loss</i> .....	8
<i>Incident Type - Penetration</i> .....	9
<i>Incident Type - Unauthorized Disclosure</i> .....	11
INCIDENTS BY TYPE OF INFORMATION EXPOSED.....	12
<i>Information Type – Personally Identifiable</i> .....	13
<i>Information Type – Social Security Numbers</i> .....	15
<i>Information Type – Medical Records</i> .....	17
<i>Information Type – Financial Records</i> .....	18
<i>Information Type – Educational Records</i> .....	19
INSTITUTIONS AFFECTED.....	20
<b>PART 3: EDUCATIONAL SECURITY INCIDENTS</b> .....	<b>22</b>
COMPUTERS STOLEN FROM UNIVERSITY MEDICAL OFFICE .....	23
HACKERS USE YALE NAME TO SPREAD WMF EXPLOIT .....	24
FOUR YEARS WORTH OF STUDENT DATA PUBLICLY ACCESSIBLE ON WEB SITE .....	25
HOTEL RESERVATION SYSTEM BREACHED.....	26
NOTRE DAME DONOR COMPUTER BREACHED .....	27
STOLEN LAPTOPS CONTAINED PATIENT MEDICAL DATA .....	28
STOLEN DESKTOP COMPUTER CONTAINS 12,000 STUDENT RECORDS .....	29
EMPLOYEE DATA AT RISK AFTER USSC COMPUTER BREACH .....	30
MASS E-MAIL EXPOSES STUDENT SOCIAL SECURITY NUMBERS .....	31
UNIVERSITY WARNS OF POSSIBLE ID THEFT AFTER W-2 INFORMATION EXPOSED .....	32
STOLEN LAPTOP USED FOR MASTERS WORK CONTAINED 93,000 STUDENT RECORDS .....	33
SECRET SERVICE INVESTIGATES GEORGETOWN COMPUTER BREACH .....	34
COMPUTER MALFUNCTION EXPOSES STUDENT RECORDS.....	35
STOLEN LAPTOP CONTAINS THOUSANDS OF STUDENT RECORDS.....	36
STOLEN LAPTOP CONTAINED INFORMATION ON VERMONT STATE COLLEGES STUDENTS, STAFF, FACULTY .....	37
GOOGLE CACHE INDEXES UNL WEB PAGE CONTAINING STUDENT INFORMATION .....	38
HACKERS ACCESS FINANCIAL DATA AT UMDNJ .....	39
MASS E-MAIL EXPOSES STUDENT SOCIAL SECURITY NUMBERS .....	40
SAN DIEGO MAN CHARGED WITH ACCESSING UNIVERSITY APPLICANTS' INFORMATION .....	41
HACKERS GET INTO UAF DATABASE .....	42
MCCOMBS SCHOOL OF BUSINESS COMPUTERS BREACHED.....	43
HUNDREDS AFFECTED BY COMPUTER THEFTS .....	44
PURDUE WARNS GRADUATE STUDENTS OVER COMPUTER BREACH.....	45
OHIO UNIVERSITY REPORTS TWO SEPARATE SECURITY BREACHES .....	46
OU'S HUDSON HEALTH CENTER SUFFERS COMPUTER SYSTEM BREACH .....	47
BREACH OF PUBLIC SAFETY COMPUTER EXPOSES MORE THEN SOCIAL SECURITY NUMBERS.....	48
GOOGLE CACHE INDEXES CSU STANISLAUS STUDENT INFORMATION.....	49
COMPUTER BREACH EXPOSES OVER 130,000 STUDENT RECORDS.....	50
FIU STUDENT RECORDS COMPROMISED BY HACKER .....	51
CURRENT AND PAST UNIVERSITY OF KENTUCKY EMPLOYEE DATA EXPOSED ONLINE.....	52
MISPLACED EQUIPMENT CONTAINS STUDENT INFORMATION .....	53

SOCIAL SECURITY NUMBERS EXPOSED OVER ELECTION DISPUTE .....	54
MORE COMPUTER BREACHES DISCOVERED AT OHIO UNIVERSITY .....	55
WESTERN ILLINOIS UNIVERSITY SECURITY BREACH EXPOSES 240,000 RECORDS.....	56
UNIVERSITY KIDNEY TRANSPLANT PROGRAM COMPUTER STOLEN .....	57
STOLEN USB DRIVE CONTAINED 18 YEARS OF STUDENT INFORMATION.....	58
LAPTOP CONTAINING 3,000 SFSU STUDENT RECORDS STOLEN .....	59
UNIVERSITY OF TENNESSEE SUFFERS COMPUTER BREACH.....	60
STOLEN LAPTOP STOLEN CONTAINS U OF I STUDENT SSNS .....	61
DATA BREACH OCCURS AT NORTHWESTERN .....	62
E-HEALTH TRIAL PUTS PATIENT DATA AT RISK.....	63
SECURITY BREACH AFFECTS PATRONS OF THE ARTS AND DOCTORAL CANDIDATES ALIKE .....	64
STOLEN LAPTOP CONTAINED SOCIAL SECURITY NUMBERS ON 3,020 PHYSICS AND ASTRONOMY STUDENTS .....	65
STOLEN LAPTOP CONTAINS EMPLOYEE INFORMATION .....	66
KENTUCKY DISCOVERS TWO INCIDENTS ON THE SAME DAY .....	67
ROGUE WiFi APs PUT DATA AT RISK .....	68
UNAUTHORIZED COMPUTER ACCESS UNCOVERED DURING USC AUDIT .....	69
GOOGLE SEARCH REVEALS PERSONAL INFORMATION .....	70
STOLEN COMPUTERS CONTAIN STUDENT INFORMATION .....	71
UNIVERSITY UNCOVERS UNAUTHORIZED ACCESS DURING ROUTINE RISK ASSESSMENT .....	72
BERRY COLLEGE "MISPLACES" SOCIAL SECURITY NUMBERS.....	73
"IDENTITY ISSUES ARE DEFINITELY AT RISK" AFTER LAPTOP THEFT.....	74
COMPUTERS MISSING FROM STORAGE CONTAINED STUDENT INFORMATION .....	75
PURDUE NOTIFIES ALUMNI OF COMPUTER BREACH.....	76
MULTIPLE LAPTOP THEFT EXPOSES PATIENT DATA.....	77
STUDENT NOTIFIED ABOUT BREACH AT A DIFFERENT UNIVERSITY.....	78
UNIVERSITY RESEARCH INFORMATION EXPOSES PARTICIPANT DATA .....	79
STOLEN LAPTOP CONTAINS INFORMATION ON ASPIRING HIGH SCHOOL STUDENTS .....	80
DONOR INFORMATION STOLEN DURING COMPUTER BREACH.....	81
YET AGAIN, STOLEN COMPUTERS CONTAIN STUDENT INFORMATION .....	82
BAD DAY FOR U OF M, PART 1.....	83
BAD DAY FOR U OF M, PART 2.....	84
COLLEGE NOTIFIES STUDENTS AND STAFF OVER FAILED INTRUSION ATTEMPT .....	85
UNIVERSITY ASSISTS MASTER'S STUDENT EVEN THOUGH BREACH DID NOT AFFECT UNIVERSITY SYSTEMS .....	86
VILLANOVA LATEST INSTITUTION AFFECTED BY LAPTOP THEFT .....	87
UNIVERSITY DELAYS NOTIFYING STUDENTS OF SSN E-MAIL MIX-UP.....	88
LAPTOP CONTAINING STUDENT INFORMATION STOLEN AND RECOVERED.....	89
E-MAIL "NOT INTENDED FOR [STUDENT] REVIEW" EXPOSES SOCIAL SECURITY NUMBERS .....	90
THIEF MAKES OFF WITH YEARS OF RESEARCH DATA.....	91
THEFT PUTS STUDENT, FACULTY IDENTITIES AT RISK.....	92
CHINESE HACK NAVAL WAR COLLEGE.....	93
THIEVES MAKE OFF WITH COMPUTERS FROM UNIVERSITY OFFICES .....	94
PRINT OUT CONTAINING 21,000 STUDENT RECORDS STOLEN.....	95
E-MAIL EXPOSES PERSONAL STUDENT INFORMATION.....	96
AUDIT FINDS STATEWIDE SYSTEM EXPOSES PRIVATE INFORMATION .....	97
UCLA BREACH EXPOSES ALMOST ONE MILLION IDENTITIES .....	98
UNIVERSITY OF TEXAS BREACH EXPOSES STUDENT AND STAFF INFORMATION .....	99
UT DALLAS ANNOUNCES BREACH IS WIDER THEN INITIALLY THOUGHT.....	100
UVA FACULTY URGED TO DESTROY ALL COMPUTER DATA AFTER RECENT INCIDENT .....	101
UC-BOULDER WEB SITE EXPLOIT EXPOSES 17,500 STUDENT RECORDS .....	102
STUDENT INFORMATION "INADVERTENTLY" LEFT EXPOSED ON PUBLIC WEBSITE.....	103
UNIVERSITY TRANSMITS 15,000 TAX FORMS OVER NON-SECURED CONNECTION .....	104
YAHOO SEARCH RETURNS FACULTY, STUDENT SOCIAL SECURITY NUMBERS.....	105

# Table of Figures

<b>Table 1: Breakdown of Incidents by Type</b>	<b>5</b>
<b>Table 2: Average Number of Records Affected Per Incident</b>	<b>5</b>
<b>Table 3: Chronological List of Theft Incidents</b>	<b>6</b>
<b>Table 4: Chronological List of Impersonation Incidents</b>	<b>7</b>
<b>Table 5: Chronological List of Loss Incidents</b>	<b>8</b>
<b>Table 6: Chronological List of Penetration Incidents</b>	<b>9</b>
<b>Table 7: Chronological List of Unauthorized Disclosure Incidents</b>	<b>11</b>
<b>Table 8: Breakdown of the Number of Incidents and Records Affected by Type of Information Exposed</b>	<b>12</b>
<b>Table 9: Breakdown of the Number of Incidents by Incident Type and Information Exposed</b>	<b>12</b>
<b>Table 10: Chronological List of Incidents Exposing Personally Identifiable Information</b>	<b>13</b>
<b>Table 11: Chronological List of Incidents Exposing Social Security Numbers</b>	<b>15</b>
<b>Table 12: Chronological List of Incidents Exposing Medical Record Information</b>	<b>17</b>
<b>Table 13: Chronological List of Incidents Exposing Financial Record Information</b>	<b>18</b>
<b>Table 14: Chronological List of Incidents Exposing Educational Record Information</b>	<b>19</b>
<b>Table 15: Alphabetical List of Institutions Affected with Number of Incidents</b>	<b>20</b>

## **Part 1: Introduction**

The Educational Security Incidents (ESI) Year in Review – 2006 is a look at the information security breaches that occurred during 2006 at colleges and universities around the world, as reported in the news. Created as a complement to the information on the ESI Web site, the ESI Year in Review – 2006 is broken into three main parts: The Introduction, Facts and Figures, and the Educational Security Incidents.

The Introduction explains the reasoning and purpose behind ESI and the ESI Year in Review – 2006 and provides background information on the goals and genesis of ESI. In addition, the Introduction also contains a set of definitions for the terms and categories used in both the Year in Review and on the ESI Web site. This first section closes with a list of sources the author and ESI use to help track information security incidents at educational institutions.

The second part of the ESI Year in Review – 2006, Facts and Figures, looks at educational security incidents in aggregate. From this total collection, Facts and Figures examines the impact different types of incidents had during 2006. The Facts and Figures part of the Year in Review also examines the impact of incidents by the types of information exposed. The final section of this second part is a run down of all institutions that reported an information security breach during 2006.

The final part of the ESI Year in Review – 2006, the Educational Security Incidents, is a collection of all information security write-ups from 2006 as collected by ESI. The write-ups are included as an easy-to-browse collection of all reported educational security incidents that occurred in 2006. In addition, the write-ups serve as evidence for the information contained in the Facts and Figures part of the Review.

## **Background**

Educational Security Incidents (ESI) is a Web site dedicated to the tracking of information security incidents that occur at colleges and universities around the world, as reported in the news. Starting as an attempt to gather example of information security breaches at educational institutions, ESI has become a niche Web site tracking and categorizing information security incidents that occur at colleges and universities. Located at <http://www.adamdodge.com/esi>, the goal of ESI is to help educational institutions understand the many threats to their information that exist.

ESI started as a personal research project with the end goal of collecting evidence that colleges and universities need to begin thinking about information security. After only a short period it became evident that information security incidents occur at educational institutions at an alarming rate. However, since numerous information security incidents are reported each week, the fact that many are educational institutions easily becomes lost. ESI was created to help illustrate and chronicle the problems college and universities face in terms of information security. The hope is that by offering a single collection and

research educational institutions will come to understand the significant threats that exist to information on college and university campuses.

ESI is a collection of abstracts pulled from reported news stories about information security incidents that occur at colleges and university around the world. The author culls these stories from a number of different sources to help build a single source for all educational information security news. The author routinely verifies the incidents contained within ESI against several well-known repositories of information security incidents to minimize the risk of missing a reported incident. A list of the Sources used by the author and ESI is provided below.

## Definitions

Each of the incidents contained within ESI follows a set formula. The report starts with a Quick Facts section that attempts to capture the bare essential information about the incident. After Quick Facts is an Abstract that summarizes the news article about the security incident.

The Quick Facts section contains the following information:

- *Date* – The date on which the incident was reported
- *Institution* – The name of the institution that suffered the incident
- *Type of Incident* – The type of incident that occurred (see below)
- *Number Affected* – The number of records affected by the incident [Please note that when speaking of a single incident a single record almost always refers to a single individual, but in total a single individuals can be represented by multiple records]
- *Source* – The source (see below) that linked to the news story [Incidents with ESI as a source were found by the author using various news searches]
- *Abstract Source* – The source of the article the abstract and quick facts are based upon

The 2006 educational security incidents are broken down between five different incident types adopted from the Classification Codes<sup>1</sup> Dr. Kabay developed for the INFOSEC Year in Review. These five types are:

- *Theft* – Incidents involving the theft of physical mediums such as drives, equipment or printouts
- *Impersonation* – Incidents involving one individual(s) masquerading as a different individual(s) or organization
- *Loss* – Incidents involving the loss of physical mediums such as drives, equipment or printouts

---

<sup>1</sup> A current list of Dr. Kabay's Classification Codes can be found at <http://www2.norwich.edu/mkabay/iyir/index.htm>

- *Penetration* – Incidents involving the breach of computer software, a computer system or a computer network
- *Unauthorized Disclosure* – Incidents involving the release of information to unknown and/or unauthorized individuals

Also included on the ESI site is a record of the type of information exposed during the incident. Colleges and universities contain vast amounts of different information on students, faculty, staff, donors and alumni. The information exposed during educational security incidents is broken down between five different types. These five types are:

- *Personally Identifiable* – Contains information that belongs to an individual, but not necessarily private such as name, address, birth date, e-mail address, etc.
- *Social Security Numbers* – The Social Security number of an individual (or the equivalent if the incident occurred outside of the United States)
- *Medical Records* – Contains the medical information of an individual
- *Financial Records* – Contains the financial information of an individual including bank accounts, checking information and credit card numbers
- *Educational Records* – Contains the educational information of an individual including class schedule and grade information

## Sources

As mentioned above, ESI collects information from a number of varied sources. Without the help of the individuals and sources list below, ESI would not be possible.

- The RISKS Forum ([catless.ncl.ac.uk/risks](http://catless.ncl.ac.uk/risks)), Dr. Peter G. Neumann, moderator
- INFOSEC Year in Review ([www2.norwich.edu/mkabay/iyir](http://www2.norwich.edu/mkabay/iyir)), Dr. M.E. Kabay, et al.
- A Chronology of Data Breaches Reported Since the ChoicePoint Incident ([www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)), Privacy Rights Clearinghouse
- Errata: Data Loss ([www.attrition.org/dataloss](http://www.attrition.org/dataloss)), Attrition.org
- Emergent Chaos ([www.emergentchaos.com](http://www.emergentchaos.com)), Adam Shostack, et al.
- InfoSec News ([www.infosecnews.org](http://www.infosecnews.org)), William Knowles, moderator
- Edupage ([www.educause.edu/Edupage/639](http://www.educause.edu/Edupage/639)), EDUCAUSE
- Security News Portal ([www.securitynewsportal.com](http://www.securitynewsportal.com))
- The thousands of newspapers and reports out there ensuring that the people know what is going on

## **Part 2: Facts and Figures**

The following part of the ESI Year in Review – 2006 breaks down the information on reported security incidents to help better examine the incidents and the effects these incidents had. Part 2 of the Year in Review – 2006 is comprised of three sections relating to different aspects of each incident: Type of Incident, Type of Information Exposed, and Institutions.

Type of Incident, breaks down the reported security incidents by the type of event that occurred. This section places each incident into one of five incident types: Theft, Impersonation, Loss, Penetration and Unauthorized Disclosure. The Type of Incident section then looks at how many incidents of each type occurred, what institutions suffered such an incident and, finally, how many records the incident affected.

The following section, Type of Information, looks at the type(s) of information exposed during the incidents. This section places each type of information exposed into one of five information types: Personally Identifiable, Social Security Numbers, Medical Information, Financial Information, and Educational Information. The Type of Information section then examines how many incidents exposed different information types as well as what the overall total is for each type of information.

The final section to the Facts and Figures part of the ESI Year in Review – 2006 is simply an alphabetical list of the 65 colleges and universities that reported suffering at least one information security breach. Along with this list is a count of the number of incidents each educational institution reported.

## Incidents by Type of Incident

In 2006, 65 different educational institutions reported 83 different educational security incidents. These 83 incidents lead to the exposure of 2,683,059 records containing at least one type of sensitive and/or personal information. This total number of records exposed includes 15 distinct incidents where there was no reporting on the number of records exposed. Below is a breakdown of the 2006 educational security incidents by the type of incident.

**Table 1: Breakdown of Incidents by Type**

Type Of Incident	Number of Incidents	Number of Institutions Affected	Number of Records Affected
Theft	26	24	237,931 <sup>2</sup>
Impersonation	1	1	<i>Unknown</i> <sup>3</sup>
Loss	3	3	4,316
Penetration	33	29	2,209,237 <sup>4</sup>
Unauthorized Disclosure	20	17	231,575 <sup>5</sup>
<b>Grand Total</b>	<b>83</b>	<b>65<sup>6</sup></b>	<b>2,683,059<sup>7</sup></b>

**Table 2: Average Number of Records Affected Per Incident**

Type Of Incident	Number of Incidents	Number of Records Affected	Average Number of Records Per Incident <sup>8</sup>
Theft	26	237,931	9,151
Impersonation	1	<i>Unknown</i>	<i>Unknown</i>
Loss	3	4,316	1,439
Penetration	33	2,209,237	66,947
Unauthorized Disclosure	20	231,575	11,579
<b>Overall Average</b>			<b>32,314</b>

<sup>2</sup> Theft total includes 4 incidents where the total number of records was not reported

<sup>3</sup> It is not known how many were affected by the Impersonation incident

<sup>4</sup> Penetration total includes 6 incidents where the total number of records was not reported

<sup>5</sup> Unauthorized Disclosure total includes 4 incidents where the total number of records was not reported

<sup>6</sup> Some institutions suffered more than one incident which is why the Grand Total for Institutions Affected does not equal the sum of the above totals

<sup>7</sup> Grand Total includes 15 incidents where the total number of records was not reported

<sup>8</sup> Rough estimates only. Averages contain calculations that include extraordinarily large incidents which may skew overall average

## Incident Type - Theft

Theft ranked as the second most common information security incident at colleges and universities as reported in the news. Overall, 24 different institutions reported 26 information security incidents related to theft of equipment, drives or printouts. These 26 incidents accounted for the exposure of 237,931 records including four incidents where the total number of records was not reported. Below is a chronological list of all Theft incidents that occurred during 2006.

**Table 3: Chronological List of Theft Incidents**

Date	Institution	Number Affected
1/1/2006	University of Pittsburg	700
1/24/2006	University of Washington	1,600
1/27/2006	College of St. Scholastica	12,000
3/3/2006	Metropolitan State College	93,000
3/24/2006	Vermont State Colleges	20,000
3/24/2006	California State University, Dominguez Hills	2,486
4/24/2006	University of Virginia	<i>Hundreds</i>
6/20/2006	University of Alabama, Birmingham	9,800
6/22/2006	University of Kentucky	6,500
6/23/2006	San Francisco State	3,000
7/14/2006	University of Iowa	280
8/1/2006	California Polytechnic State University	3,020
8/2/2006	Belhaven College	300
9/8/2006	University of Minnesota	13,084
9/20/2006	University of Wisconsin, Whitewater	<i>Unknown</i>
9/24/2006	Nagasaki University	9,000
10/11/2006	Adams State College	184
10/12/2006	University of Texas, Austin	2,500
10/20/2006	University of Minnesota	200
10/20/2006	University of Minnesota	13,000
11/2/2006	Villanova University	1,243
11/14/2006	Connors State College	22,500
11/23/2006	University of Colorado, Boulder	<i>Unknown</i>
11/28/2006	California State, Los Angeles	2,534
12/4/2006	Troy University	<i>Unknown</i>
12/5/2006	Nassau Community College	21,000
	<b>Total</b>	<b>237,931<sup>9</sup></b>

<sup>9</sup> Total for Theft-type incidents includes 4 incidents where the total number of records was not reported

## Incident Type - Impersonation

Impersonation ranked as the least common information security incident at colleges and universities as reported in the news. Overall, one institution reported a single case of Impersonation. At the time reported, it was unknown how many were affected by this single incident. Below is a chronological list of the Impersonation incident that occurred during 2006.

**Table 4: Chronological List of Impersonation Incidents**

<b>Date</b>	<b>Institution</b>	<b>Number Affected</b>
1/9/2006	Yale University	<i>Unknown</i>
	<b>Total</b>	<b><i>Unknown</i><sup>10</sup></b>

---

<sup>10</sup> Total for Impersonation-type incidents was not reported

## Incident Type - Loss

Loss ranked as the second least common information security incident at colleges and universities as reported in the news. Overall, three different institutions reported three information security incidents related to loss of equipment, drives or printouts. These three incidents accounted for the exposure of 4,316 records. Below is a chronological list of all Loss incidents that occurred during 2006.

**Table 5: Chronological List of Loss Incidents**

<b>Date</b>	<b>Institution</b>	<b>Number Affected</b>
6/1/2006	Miami University	851
9/20/2006	Berry College	2,093
9/22/2006	University of Colorado, Boulder	1,372
	<b>Total</b>	<b>4,316</b>

## Incident Type - Penetration

Penetration ranked as the most common information security incident at colleges and universities as reported in the news. Overall, 29 different institutions reported 33 information security incidents related to breaching of computers and networks. These 33 incidents accounted for the exposure of 2,209,237 records including six incidents where the total number of records was not reported. Below is a chronological list of all Penetration incidents that occurred during 2006.

**Table 6: Chronological List of Penetration Incidents**

<b>Date</b>	<b>Institution</b>	<b>Number Affected</b>
1/21/2006	Indiana University	<i>Unknown</i>
1/23/2006	Notre Dame	<i>Unknown</i>
2/1/2006	University of Colorado, Silver Springs	2,500
2/18/2006	University of Northern Iowa	6,000
3/6/2006	Georgetown University	41,000
4/9/2006	University of Medicine and Dentistry of New Jersey	1,850
4/21/2006	University of Alaska, Fairbanks	39,000
4/21/2006	University of Southern California	275,000
4/26/2006	Purdue University	1,351
5/2/2006	Ohio University	300,000
5/12/2006	Ohio University	60,000
5/16/2006	University of California, Berkeley	1,200
5/23/2006	University of Delaware	1,076
5/26/2006	Sacred Hart University	130,000
5/31/2006	Florida International University	<i>Unknown</i>
6/6/2006	University of Texas, El Paso	4,719
6/9/2006	Ohio University	70,000
6/17/2006	Western Illinois University	240,000
7/6/2006	University of Tennessee	36,000
7/14/2006	Northwestern University	17,000
8/1/2006	Wichita State University	2,040
8/26/2006	University of South Carolina	6,000
9/15/2006	University of Texas, San Antonio	64,000

9/22/2006	Purdue University	2,500
9/27/2006	Scared Hart University	<i>Unknown</i>
9/29/2006	University of Iowa	14,500
10/12/2006	Brock University	70,000
10/28/2006	St. Norbert College	<i>Unknown</i>
10/29/2006	Nanyang Technological University	1
11/30/2006	Naval War College	<i>Unknown</i>
12/12/2006	University of California, Los Angeles	800,000
12/12/2006	University of Texas, Dallas	6,000
	<b>Total</b>	<b>2,209,237<sup>11</sup></b>

---

<sup>11</sup> Total for Penetration-type incidents includes 6 incidents where the total number of records was not reported.

## Incident Type - Unauthorized Disclosure

Unauthorized Disclosure ranked as the third most common information security incident at colleges and universities as reported in the news. Overall, 17 different institutions reported 20 information security incidents related to the distribution of information to unknown and/or unauthorized individuals. These 20 incidents accounted for the exposure of 231,575 records including four incidents that affected an unknown number. Below is a chronological list of all Penetration incidents that occurred during 2006.

**Table 7: Chronological List of Unauthorized Disclosure Incidents**

Date	Institution	Number Affected
1/20/2006	Kansas University	<i>Unknown</i>
2/15/2006	Old Dominion University	601
3/20/2006	Canterbury University	<i>Unknown</i>
3/29/2006	University of Nebraska-Lincoln	342
4/14/2006	University of South Carolina	1,400
4/24/2006	University of Texas, Austin	197,000
5/26/2006	California State University, Stanislaus	1,294
6/1/2006	University of Kentucky	1,300
7/25/2006	Georgetown University	23,000
8/15/2006	University of Kentucky	710
8/25/2006	University of Iowa	<i>Unknown</i>
9/1/2006	Virginia Commonwealth University	2,100
11/3/2006	University of Virginia	632
11/17/2006	Jefferson College of Health Science	143
12/9/2006	Virginia Commonwealth University	591
12/11/2006	North Dakota University System	<i>Unknown</i>
12/14/2006	University of Virginia	62
12/19/2006	Mississippi State University	2,400
12/22/2006	Texas Woman's University	15,000
12/22/2006	Utah Valley State College	15,000
	<b>Total</b>	<b>231,575<sup>12</sup></b>

<sup>12</sup> Total for Unauthorized Disclosure-type incidents includes 4 incidents where the total number of records was not reported.

## Incidents by Type of Information Exposed

The Type of Information Exposed section looks the types of information the security incidents at colleges and universities exposed. Below is a breakdown of the number of incidents and total number of records affected by the type of information exposed during a breach. The total number of records affected in this section is higher then in the Type of Incident section for good reason.

In the Type of Incident section, each “record” represented a collection of information records about an individual. In this section, the each “record” represents a specific piece of information about an individual. Therefore, each Type of Incident record could contain multiple Type of Information records.

**Table 8: Breakdown of the Number of Incidents and Records Affected by Type of Information Exposed**

Type of Information	Number of Incidents	Number of Records Affected
Personally Identifiable	76	2,648,059 <sup>13</sup>
Social Security Number	66	2,268,580 <sup>14</sup>
Medical Records	5	80,400 <sup>15</sup>
Financial Records	13	161,283 <sup>16</sup>
Educational Records	1	342

Below is a quick breakdown of the number of incidents in each type of incident by the type of information these incidents exposed. Any field marked with a dash (-) represents an area where no educational institution reported a loss of the type of information by that type of incident. For example, no college or university reported the exposure of Medical Record information due to the Loss of computers, disks or printouts.

**Table 9: Breakdown of the Number of Incidents by Incident Type and Information Exposed**

Type of Information	Theft	Impersonation <sup>17</sup>	Loss	Penetration	Unauthorized Disclosure
Personally Identifiable	24	-	3	30	19
Social Security Numbers	19	-	2	26	19
Medical	3	-	-	1	1
Financial	1	-	1	7	4
Educational	-	-	-	-	1

<sup>13</sup> Personally Identifiable total includes 9 incidents where the total number of records was not reported

<sup>14</sup> Social Security Number total includes 7 incidents where the total number of records was not reported

<sup>15</sup> Medical Record total includes one incident where the total number of records was not reported

<sup>16</sup> Financial Record total includes 5 incidents where the total number of records was not reported

<sup>17</sup> Little is known about the effects of the Yale Impersonation incident

## Information Type – Personally Identifiable

Personally Identifiable information ranked as the most common type of information exposed by information security incidents at colleges and universities as reported in the news. Overall, 76 information security incidents exposed 2,648,059 records containing Personally Identifiable information such as names, dates of birth, addresses, and e-mail addresses including nine incidents where the number exposed was not reported. Below is a chronological list of all incidents exposing Personally Identifiable information that occurred during 2006.

**Table 10: Chronological List of Incidents Exposing Personally Identifiable Information**

Date	Institution	Number Affected
1/1/2006	University of Pittsburgh	700
1/20/2006	Kansas University	<i>Unknown</i>
1/21/2006	Indiana University	<i>Unknown</i>
1/23/2006	Notre Dame	<i>Unknown</i>
1/24/2006	University of Washington	1,600
1/27/2006	College of St. Scholastica	12,000
2/1/2006	University of Colorado, Silver Springs	2,500
2/15/2006	Old Dominion University	601
2/18/2006	University of Northern Iowa	6,000
3/3/2006	Metropolitan State College	93,000
3/6/2006	Georgetown University	41,000
3/20/2006	Canterbury University	<i>Unknown</i>
3/24/2006	Vermont State Colleges	20,000
3/24/2006	California State University, Dominguez Hills	2,486
3/29/2006	University of Nebraska-Lincoln	342
4/9/2006	University of Medicine and Dentistry of New Jersey	1,850
4/14/2006	University of South Carolina	1,400
4/21/2006	University of Southern California	275,000
4/21/2006	University of Alaska, Fairbanks	39,000
4/24/2006	University of Virginia	<i>Hundreds</i>
4/24/2006	University of Texas, Austin	197,000
4/26/2006	Purdue University	1,351
5/2/2006	Ohio University	300,000
5/12/2006	Ohio University	60,000
5/16/2006	University of California, Berkeley	1,200
5/23/2006	University of Delaware	1,076
5/26/2006	Sacred Heart University	135,000
5/26/2006	California State University, Stanislaus	1,294
5/31/2006	Florida International University	<i>Unknown</i>
6/1/2006	Miami University	851
6/1/2006	University of Kentucky	1,300
6/6/2006	University of Texas, El Paso	4,719
6/17/2006	Western Illinois University	240,000
6/20/2006	University of Alabama, Birmingham	9,800
6/22/2006	University of Kentucky	6,500
6/23/2006	San Francisco State	3,000
7/6/2006	University of Tennessee	36,000

7/14/2006	Northwestern University	17,000
7/14/2006	University of Iowa	280
7/25/2006	Georgetown University	23,000
8/1/2006	Wichita State University	2,040
8/1/2006	California Polytechnic State University	3,020
8/2/2006	Belhaven College	300
8/15/2006	University of Kentucky	710
8/26/2006	University of South Carolina	6,000
9/1/2006	Virginia Commonwealth University	2,100
9/8/2006	University of Minnesota	13,084
9/15/2006	University of Texas, San Antonio	64,000
9/20/2006	Berry College	2,093
9/20/2006	University of Wisconsin, Whitewater	<i>Unknown</i>
9/22/2006	University of Colorado, Boulder	1,372
9/22/2006	Purdue University	2,500
9/24/2006	Nagasaki University	9,000
9/27/2000	Sacred Heart University	<i>Unknown</i>
9/29/2006	University of Iowa	14,500
10/11/2006	Adams State College	184
10/12/2006	Brock University	70,000
10/12/2006	University of Texas, Austin	2,500
10/20/2006	University of Minnesota	13,000
10/20/2006	University of Minnesota	200
10/29/2006	Nanyang Technological University	1
11/2/2006	Villanova University	1,243
11/3/2006	University of Virginia	632
11/14/2006	Connors State College	22,500
11/17/2006	Jefferson College of Health Sciences	143
11/28/2006	California State, Los Angeles	2,534
12/5/2006	Nassau Community College	21,000
12/9/2006	Virginia Commonwealth University	591
12/11/2006	North Dakota University System	<i>Unknown</i>
12/12/2006	University of Texas, Dallas	6,000
12/12/2006	University of California, Los Angeles	800,000
12/14/2006	University of Virginia	62
12/15/2006	University of Colorado, Boulder	17,500
12/19/2006	Mississippi State University	2,400
12/22/2006	Texas Woman's University	15,000
12/22/2006	Utah Valley State College	15,000
	<b>Total</b>	<b>2,648,059<sup>18</sup></b>

<sup>18</sup> Number of records affected for Personally Identifiable Information includes 9 incidents where the total number of records affected was not reported

## Information Type – Social Security Numbers

Social Security Numbers (or the non-US equivalent) ranked as the second most common type of information exposed by information security incidents at colleges and universities as reported in the news. Overall, 66 information security incidents exposed 2,268,580 records containing Social Security numbers or the government identification numbers of a non-US country including seven incidents where the number affected was not reported. Below is a chronological list of all incidents exposing Social Security numbers or the non-US equivalent that occurred during 2006.

**Table 11: Chronological List of Incidents Exposing Social Security Numbers**

Date	Institution	Number Affected
1/1/2006	University of Pittsburgh	700
1/20/2006	Kansas University	<i>Unknown</i>
1/23/2006	Notre Dame	<i>Unknown</i>
1/24/2006	University of Washington	1,600
1/27/2006	College of St. Scholastica	12,000
2/1/2006	University of Colorado, Silver Springs	2,500
2/15/2006	Old Dominion University	601
2/18/2006	University of Northern Iowa	6,000
3/3/2006	Metropolitan State College	93,000
3/6/2006	Georgetown University	41,000
3/20/2006	Canterbury University	<i>Unknown</i>
3/24/2006	Vermont State Colleges	20,000
3/24/2006	California State University, Dominguez Hills	2,486
3/29/2006	University of Nebraska-Lincoln	342
4/9/2006	University of Medicine and Dentistry of New Jersey	1,850
4/14/2006	University of South Carolina	1,400
4/21/2006	University of Alaska, Fairbanks	39,000
4/21/2006	University of Southern California	275,000
4/24/2006	University of Virginia	<i>Hundreds</i>
4/24/2006	University of Texas, Austin	197,000
4/26/2006	Purdue University	1,351
5/2/2006	Ohio University	137,000
5/12/2006	Ohio University	60,000
5/16/2006	University of California, Berkeley	1,200
5/23/2006	University of Delaware	1,076
5/26/2006	California State University, Stanislaus	1,294
5/31/2006	Florida International University	<i>Unknown</i>
6/1/2006	University of Kentucky	1,300
6/6/2006	University of Texas, El Paso	4,719
6/17/2006	Western Illinois University	240,000
6/20/2006	University of Alabama, Birmingham	9,800
6/22/2006	University of Kentucky	6,500
6/23/2006	San Francisco State	3,000
7/6/2006	University of Tennessee	36,000
7/14/2006	Northwestern University	17,000
7/14/2006	University of Iowa	280

7/25/2006	Georgetown University	23,000
8/1/2006	Wichita State University	2,040
8/1/2006	California Polytechnic State University	3,020
8/2/2006	Belhaven College	300
8/15/2006	University of Kentucky	710
8/26/2006	University of South Carolina	6,000
9/1/2006	Virginia Commonwealth University	2,100
9/8/2006	University of Minnesota	13,084
9/15/2006	University of Texas, San Antonio	64,000
9/20/2006	Berry College	2,093
9/22/2006	Purdue University	2,500
9/22/2006	University of Colorado, Boulder	1,372
9/27/2000	Sacred Heart University	<i>Unknown</i>
9/29/2006	University of Iowa	14,500
10/12/2006	University of Texas, Austin	2,500
10/20/2006	University of Minnesota	13,000
11/3/2006	University of Virginia	632
11/14/2006	Connors State College	22,500
11/17/2006	Jefferson College of Health Sciences	143
11/28/2006	California State, Los Angeles	2,534
12/5/2006	Nassau Community College	21,000
12/9/2006	Virginia Commonwealth University	591
12/11/2006	North Dakota University System	<i>Unknown</i>
12/12/2006	University of Texas, Dallas	6,000
12/12/2006	University of California, Los Angeles	800,000
12/14/2006	University of Virginia	62
12/15/2006	University of Colorado, Boulder	17,500
12/19/2006	Mississippi State University	2,400
12/22/2006	Texas Woman's University	15,000
12/22/2006	Utah Valley State College	15,000
	<b>Total</b>	<b>2,268,580<sup>19</sup></b>

<sup>19</sup> Total number of records containing Social Security numbers or the non-US equivalent includes 7 incidents where the total number of records affected was not reported

## Information Type – Medical Records

Medical Records information ranked as the second least common type of information exposed by information security incidents at colleges and universities as reported in the news. Overall, 5 information security incidents exposed 80,400 records containing Medical Records information such as diagnosis and treatment information including one incident where the number affected was not reported. Below is a chronological list of all incidents exposing Medical Records information that occurred during 2006.

**Table 12: Chronological List of Incidents Exposing Medical Record Information**

<b>Date</b>	<b>Institution</b>	<b>Number Affected</b>
1/24/2006	University of Washington	1,600
3/20/2006	Canterbury University	<i>Unknown</i>
5/12/2006	Ohio University	60,000
6/20/2006	University of Alabama, Birmingham	9,800
9/24/2006	Nagasaki University	9,000
	<b>Total</b>	<b>80,400<sup>20</sup></b>

---

<sup>20</sup> Total number of records containing Medical Records information includes 1 incident where the total number was not reported.

## Information Type – Financial Records

Financial Records information ranked as the third most common type of information exposed by information security incidents at colleges and universities as reported in the news. Overall, 13 information security incidents exposed 160,983 records containing Financial Records information such as credit card and bank account numbers including 6 incidents where the number affected was not reported. Below is a chronological list of all incidents exposing Financial Records information that occurred during 2006.

**Table 13: Chronological List of Incidents Exposing Financial Record Information**

<b>Date</b>	<b>Institution</b>	<b>Number Affected</b>
1/20/2006	Kansas University	<i>Unknown</i>
1/21/2006	Indiana University	<i>Unknown</i>
1/23/2006	Notre Dame	<i>Unknown</i>
2/18/2006	University of Northern Iowa	6,000
3/20/2006	Canterbury University	<i>Unknown</i>
4/9/2006	University of Medicine and Dentistry of New Jersey	1,850
8/1/2006	Wichita State University	2,040
9/15/2006	University of Texas, San Antonio	64,000
9/20/2006	Berry College	2,093
10/12/2006	Brock University	70,000
12/11/2006	North Dakota University System	<i>Unknown</i>
12/22/2006	Texas Woman's University	15,000
1/20/2006	Kansas University	<i>Unknown</i>
	<b>Total</b>	<b>160,983<sup>21</sup></b>

<sup>21</sup> Total number of records containing Financial Records information includes 6 incident where the total number was not reported.

## Information Type – Educational Records

Educational Records information ranked as the least common type of information exposed by information security incidents at colleges and universities as reported in the news. Overall, 1 information security incident exposed 342 records containing Educational Records information such student grades and class schedules. Below is a chronological list of all incidents exposing Educational Records information that occurred during 2006.

**Table 14: Chronological List of Incidents Exposing Educational Record Information**

<b>Date</b>	<b>Institution</b>	<b>Number Affected</b>
3/29/2006	University of Nebraska-Lincoln	342
	<b>Total</b>	<b>342</b>

## Institutions Affected

During 2006, 83 different information security incidents occurred at 65 different colleges and universities. 57 of these 65 institutions reported to suffer only a single security breach. However, six institutions suffered two breaches while five college and universities reported three information security incidents. Below is an alphabetical list of all 65 colleges and universities along with the number of information security incidents the institution suffered.

**Table 15: Alphabetical List of Institutions Affected with Number of Incidents**

Institutions	Number of Incidents
Adams State College	1
Belhaven College	1
Berry College	1
Brock University	1
California Polytechnic State University	1
California State University, Dominguez Hills	1
California State University, Stanislaus	1
California State, Los Angeles	1
Canterbury University	1
College of St. Scholastica	1
Connors State College	1
Florida International University	1
Georgetown University	2
Indiana University	1
Jefferson College of Health Science	1
Kansas University	1
Metropolitan State College	1
Miami University	1
Mississippi State University	1
Nagasaki University	1
Nanyang Technological University	1
Nassau Community College	1
Naval War College	1
North Dakota University System	1
Northwestern University	1
Notre Dame	1
Ohio University	3
Old Dominion University	1
Purdue University	2
Sacred Hart University	2
San Francisco State	1
St. Norbert College	1
Texas Woman's University	1
Troy University	1

University of Alabama, Birmingham	1
University of Alaska, Fairbanks	1
University of California, Berkeley	1
University of California, Los Angeles	1
University of Colorado, Boulder	3
University of Colorado, Silver Springs	1
University of Delaware	1
University of Iowa	3
University of Kentucky	3
University of Medicine and Dentistry of New Jersey	1
University of Minnesota	3
University of Nebraska-Lincoln	1
University of Northern Iowa	1
University of Pittsburg	1
University of South Carolina	2
University of Southern California	1
University of Tennessee	1
University of Texas, Austin	2
University of Texas, Dallas	1
University of Texas, El Paso	1
University of Texas, San Antonio	1
University of Virginia	3
University of Washington	1
University of Wisconsin, Whitewater	1
Utah Valley State College	1
Vermont State Colleges	1
Villanova University	1
Virginia Commonwealth University	2
Western Illinois University	1
Wichita State University	1
Yale University	1
<b>Total</b>	<b>83</b>

## Part 3: Educational Security Incidents

The third and final part of the ESI Year in Review – 2006 is a collection of all of the educational security incidents that appear on the ESI web site for 2006. The incident write-ups contain the following parts: Title, Quick Facts, Abstract, and Links. These different parts exist to help provide a good overview of the incident and links to more information. Below is a brief description of each part:

- *Title* – A one line description of the incident
- *Quick Facts* – A snapshot that captures all pertinent information in one quick list
- *Abstract* – A more detailed analysis of the incident pulled from the news article listed in the Quick Fact
- *Links* – Web site address corresponding to hyperlinks that exist in the online version of the incident write-up

A quick note on the Links: Each of these links was active at the time of the incident write-up. Given the fluid nature of the Internet, there is no guarantee that these links remain active. While it is most likely that these links are still valid; there have been no attempts by ESI or the author to verify this fact.

## Computers Stolen From University Medical Office

### Quick Facts

- Date: 1/1/2006
- Institution: University of Pittsburgh [1]
- Type of Incident: Theft
- Number Affected: 700
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: Pittsburgh Post Gazette [3]

### Abstract

In December, six computers were stolen from the University of Pittsburgh Medical Center's (UPMC) Squirrel Hill Family Medicine office. These computer contained names, Social Security Numbers and birthdates on as many as 700 patients. The University was quick to point out that the data compromised was "not information about health care, not information about their medical conditions". In a letter sent on December 20, UPMC notified the patients of the break-in and offered to help

---

### Links:

[1] <http://www.pitt.edu>

[2] <http://www.privacyrights.org>

[3] <http://www.post-gazette.com/pg/06001/630909.stm>

# Hackers Use Yale Name To Spread WMF Exploit

## Quick Facts

- Date: 1/9/2006
- Institution: Yale University [1]
- Type of Incident: Impersonation
- Number Affected: Unknown
- Source: InfoSec News [2]
- Abstract Source: Yale Daily News [3]

## Abstract

A forged e-mail address of a Yale professor was used by hackers to spread a variant of the WMF exploit. The e-mail attempts to fool recipients into clicking on an included hypertext link. The e-mail is from a factious "Professor Robert Gordens" and asks the recipients for help in catching a graffiti vandal. Yale has not been linked to this WMF attack but has already received over 30 complaints from British citizens.

---

## Links:

[1] <http://www.yale.edu>

[2] <http://www.infosecnews.org>

[3] <http://www.yaledailynews.com/article.asp?AID=31167>

# Four Years Worth of Student Data Publicly Accessible on Web Site

## Quick Facts

- Date: 1/20/2006
- Institution: [Kansas University](#) [1]
- Type of Incident: Unauthorized disclosure
- Number Affected: Unknown
- Source: [InfoSec News](#) [2]
- Abstract Source: [The Kansan](#) [3]

## Abstract

Students who utilized the KU online housing application system were notified that their private information might have been exposed. Kansas University found that a file containing names, addresses, birth dates, phone numbers, Social Security numbers and credit card number was accessible to the public December 16, 2005. These records exists for any student who used the online application between April 29, 2001 and December 16, 2005.

---

## Links:

[1] <http://www.kansas.edu>

[2] <http://www.infosecnews.org>

[3] <http://www.kansan.com/stories/2006/jan/20/hack/>

# Hotel Reservation System Breached

## Quick Facts

- Date: 1/21/2006
- Institution: [Indiana University](http://www.indiana.edu) [1]
- Type of Incident: Penetration
- Number Affected: Unknown
- Source: [Privacy Rights Clearinghouse](http://www.privacyrights.org) [2]
- Abstract Source: [Privacy Rights Clearinghouse Chronology of Data Breaches](http://www.privacyrights.org/ar/ChronDataBreaches.htm) [3]

## Abstract

On Jan 21 an unknown number of credit card numbers was exposed when the reservation system of Indiana University's University Place Conference Center and Hotel was compromised.

Abstract by Privacy Rights Clearinghouse Editors

---

## Links:

[1] <http://www.indiana.edu>

[2] <http://www.privacyrights.org>

[3] <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

# Notre Dame Donor Computer Breached

## Quick Facts

- Date: 1/23/2006
- Institution: Notre Dame [1]
- Type of Incident: Penetration
- Number Affected: Unknown
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: C|Net News.com [3]

## Abstract

Notre Dame is investigating the compromise of a computer containing financial information from school donors. During the compromise, names, address, Social Security numbers, credit card numbers and check images on an undisclosed number of past and current donors.

---

## Links:

[1] <http://www.nd.edu>

[2] <http://www.privacyrights.org>

[3] [http://news.com.com/Notre+Dame+probes+hack+of+computer+system/2100-1029\\_3-6030229.html](http://news.com.com/Notre+Dame+probes+hack+of+computer+system/2100-1029_3-6030229.html)

## Stolen Laptops Contained Patient Medical Data

### Quick Facts

- Date: 1/24/2006
- Institution: University of Washington [1]
- Type of Incident: Theft
- Number Affected: 1,600
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: Seattle Post-Intelligencer [3]

### Abstract

Two laptops containing 1,600 patient records were stolen from a UW Medical Center off-campus office. Contained on these laptops were names, addresses, Social Security numbers, maiden names, birth dates, diagnosis and other personal data. Only one of these laptops protected this information with password access. The University also released that no detailed medical records were disclosed due to this theft.

---

### Links:

[1] <http://www.washington.edu>

[2] <http://www.privacyrights.org>

[3] [http://seattlepi.nwsourc.com/local/256774\\_laptop24.html](http://seattlepi.nwsourc.com/local/256774_laptop24.html)

## Stolen Desktop Computer Contains 12,000 Student Records

### Quick Facts

- Date: 01/27/2006
- Institution: College of St. Scholastica [1]
- Type of Incident: Theft
- Number Affected: 12,000
- Source: Attrition.org [2]
- Abstract Source: Duluth News Tribune [3]

### Abstract

A desktop computer was recently stolen from a locked office within the College of St. Scholastica's Information Technology Department. The names and Social Security numbers of 12,000 CSS students were stored on this computer. While CSS has since retrieved the computer, there is still a chance the information might have been accessed. CSS does not believe that anyone did, in fact, access this information but is alerting affected student just to be safe. CSS urges any affected student to monitor their credit reports for unusual behavior.

---

### Links:

[1] <http://www.css.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.duluthsuperior.com/mld/duluthsuperior/13730388.htm>

## Employee Data At Risk After USSC Computer Breach

### Quick Facts

- Date: 02/01/2006
- Institution: [University of Colorado, Silver Springs](#) [1]
- Type of Incident: Penetration
- Number Affected: 2,500
- Source: [Attrition.org](#) [2]
- Abstract Source: [The Gazette](#) [3]

### Abstract

University of Colorado at Silver Springs announced it uncovered a recent computer breach in the Personnel Department. The unknown intruder gained access to one of seven Personnel Department computers containing the names, Social Security numbers, dates of birth and addresses on 2,500 employees dating back to 2004. There is no evidence that the goal of the attack was to gain this information. However, USSC urges all affected employees to alert credit agencies and monitor their credit reports.

---

### Links:

[1] <http://www.uccs.edu/>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.gazette.com/display.php?id=1314249&secid=1>

# Mass E-mail Exposes Student Social Security Numbers

## Quick Facts

- Date: 2/15/2006
- Institution: [Old Dominion University](#) [1]
- Type of Incident: Unauthorized disclosure
- Number Affected: 601
- Source: [Privacy Rights Clearinghouse](#) [2]
- Abstract Source: [Privacy Rights Clearinghouse Chronology of Data Breaches](#) [3]

## Abstract

A professor accidentally exposed the names and Social Security numbers of 601 Old Dominion University students when a class roster was posted on the class website.

Abstract by Privacy Rights Clearinghouse Editors

---

## Links:

[1] <http://www.odu.edu>

[2] <http://www.privacyrights.org>

[3] <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

## University Warns of Possible ID Theft After W-2 Information Exposed

### Quick Facts

- Date: 2/18/2006
- Institution: University of Northern Iowa [1]
- Type of Incident: Penetration
- Number Affected: 6,000
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: WCF Courier [3]

### Abstract

A computer breach at the University of Northern Iowa prompted UNI to notify 6,000 student employees and faculty that their W-2 tax forms might have been exposed. UNI issued immediate warnings for these individuals to "monitor their bank accounts" following the security breach.

---

### Links:

[1] <http://www.uni.edu>

[2] <http://www.privacyrights.org>

[3]

[http://www.wcfcourier.com/articles/2006/02/18/news/breaking\\_news/doc43f7026269046987392075.html](http://www.wcfcourier.com/articles/2006/02/18/news/breaking_news/doc43f7026269046987392075.html)

# Stolen Laptop Used For Masters Work Contained 93,000 Student Records

## Quick Facts

- Date: 3/3/2006
- Institution: Metropolitan State College [1]
- Type of Incident: Theft of equipment
- Number Affected: 93,000
- Source: InfoSec News [2]
- Abstract Source: ComputerWorld [3]

## Abstract

A laptop containing sensitive information on over 93,000 students was stolen from a Denver state college employee's home. The Metropolitan State College employee was using the student information to prepare a grant request and as part of the employee's master's degree thesis. All students who had registered for courses between the fall semester of 1996 and the summer semester of 2005 could be affected by this theft. While the college is notifying students of the potential exposure, a number of individuals are asking why this information was not encrypted as well as why an employee was allowed to use sensitive student information in a thesis.

---

## Links:

[1] <http://www.metrostate.edu>

[2] <http://www.infosecnews.org>

[3] <http://www.computerworld.com/securitytopics/security/story/0,10801,109208,00.html>

# Secret Service Investigates Georgetown Computer Breach

## Quick Facts

- Date: 3/6/2006
- Institution: [Georgetown University](#) [1]
- Type of Incident: Penetration
- Number Affected: 41,000
- Source: [InfoSec News](#) [2]
- Abstract Source: [ComputerWorld](#) [3]

## Abstract

The US Secret Service has been called in to investigate the breach of a Georgetown University server that contained the names, dates of birth, and Social Security numbers of more than 41,000 people. The server was part of a grant project to manage information on various services provided by the Office of Aging in the District of Columbia. The breach was first noticed on Feb 12 by the Georgetown information security office. Georgetown notified the Office for the Aging on Feb 24 after the University understood the full scope of the exposure. The Secret Service was brought in on Feb 27 to aid in the investigation. The server in question was run and administered by an individual researcher and not by Georgetown University.

---

## Links:

[1] <http://www.georgetown.edu>

[2] <http://www.infosecnews.org>

[3]

<http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,109245,00.html>

# Computer Malfunction Exposes Student Records

## Quick Facts

- Date: 3/20/2006
- Institution: [Canterbury University](#) [1]
- Type of Incident: Unauthorized disclosure
- Number Affected:
- Source: [INFOSEC Year In Review](#) [2]
- Abstract Source: [RISKS 24.17](#) [3]

## Abstract

(Abstract by Andrew King, taken from RISKS 24.17)

Thousands of [AU] Canterbury University students had their personal information exposed when online services were shut down leaving private records available to anyone with a user code and password last night. Information such as IRD numbers, transcripts, results, outstanding payments, medical conditions, and personal addresses could all be easily accessed online and could be changed by system users. The university's information technology department shut down the web front. The university had installed a new online system late last year but there had not been any problems until now.

[Source: \*New Zealand Herald\*, 20 Feb 2006; PGN-ed]

[http://www.nzherald.co.nz/section/story.cfm?c\\_id=1&ObjectID=10369269](http://www.nzherald.co.nz/section/story.cfm?c_id=1&ObjectID=10369269)

---

## Links:

[1] <http://www.canterbury.ac.nz>

[2] <http://www2.norwich.edu/mkabay/iyir/>

[3] <http://catless.ncl.ac.uk/Risks/24.17.html#subj6.1>

# Stolen Laptop Contains Thousands of Student Records

## Quick Facts

- Date: 03/24/2006
- Institution: California State University, Dominguez Hills [1]
- Type of Incident: Theft
- Number Affected: 2,486
- Source: Attrition.org [2]
- Abstract Source: California State University, Dominguez Hills [3]

## Abstract

A laptop belonging to a CSU, Dominguez Hills professor was recently stolen from the professor's office. This laptop contained information on 2,486 current and potential students that were completely separate from any other CSU, Dominguez Hills database. The university has no evidence that the information contained on the laptop was the target and believe the thief was only after a computer. However, the university has created a web site - www.csudh.edu/securityinfo [4] - for students that have questions about the theft.

---

## Links:

[1] <http://www.csudh.edu/>

[2] <http://www.attrition.org/dataloss>

[3] [http://www.csudh.edu/univadv/Newsroom/2006/DH06\\_RH24.html](http://www.csudh.edu/univadv/Newsroom/2006/DH06_RH24.html)

[4] <http://www.csudh.edu/securityinfo>

## Stolen Laptop Contained Information on Vermont State Colleges Students, Staff, Faculty

### Quick Facts

- Date: 3/24/2006
- Institution: Vermont State Colleges [1]
- Type of Incident: Theft
- Number Affected: 20,000
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: Boston.com(Free Reg. Required) [3]

### Abstract

A laptop stolen from the car of Vermont State Colleges' Chief Information Officer (CIO) contained six years of personal information on faculty, staff and current and past students. The computer contained names, address, birth dates and Social Security numbers. As many as 20,000 individuals could have been exposed. VSC has sent out letters out to 50,000 current and former students and employees alerting them to this theft.

---

### Links:

[1] <http://www.vsc.edu>

[2] <http://www.privacyrights.org>

[3]

[http://www.boston.com/news/local/vermont/articles/2006/04/06/colleges\\_say\\_no\\_signs\\_identity\\_theft\\_from\\_stolen\\_laptop](http://www.boston.com/news/local/vermont/articles/2006/04/06/colleges_say_no_signs_identity_theft_from_stolen_laptop)

# Google Cache Indexes UNL Web Page Containing Student Information

## Quick Facts

- Date: 03/29/2006
- Institution: [University of Nebraska-Lincoln](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 342
- Source: [Attrition.org](#) [2]
- Abstract Source: [Technology Marketing Corporation](#) [3]

## Abstract

The University of Nebraska-Lincoln is tightening its information security posture after it was discovered that the Google search engine's Google Cache service had stored a UNL College of Engineering Web page that contained information. This page was used in 2004 by the College of Engineering to track student information contained student names, e-mail address, Social Security numbers and grade point averages. UNL had removed this page from its servers earlier in 2006, but Google Cache had already indexed the page.

---

## Links:

[1] <http://www.unl.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.tmcnet.com/usubmit/2006/03/29/1518938.htm>

## Hackers Access Financial Data at UMDNJ

### Quick Facts

- Date: 4/9/2006
- Institution: University of Medicine and Dentistry of New Jersey [1]
- Type of Incident: Penetration
- Number Affected: 1,850
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: WCBS, New York, NY [3]

### Abstract

Computer attackers gained access to Social Security numbers and financial information on 1,850 University of Medicine and Dentistry of New Jersey students and alumni. UMDNJ was able to determine that the personal information was accessed by the attackers but could not verify if any of the information was copied. The interim dean of UMDNJ's Medical School sent letters to students notifying them about the security breach.

---

### Links:

[1] <http://www.umdj.edu>

[2] <http://www.privacyrights.org>

[3] [http://wcbstv.com/topstories/local\\_story\\_099123340.html](http://wcbstv.com/topstories/local_story_099123340.html)

# Mass E-mail Exposes Student Social Security Numbers

## Quick Facts

- Date: 4/14/2006
- Institution: University of South Carolina [1]
- Type of Incident: Unauthorized disclosure
- Number Affected: 1,400
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: MSNBC [3]

## Abstract

An e-mail mistakenly sent to University of South Carolina students contained the Social Security numbers and names of 1,400 classmates. The department chairwoman accidentally attached this information at an e-mail sent to all students participating in the summer semester at USC. The school has notified all students of the problem and advises that they watch their credit reports for odd behavior.

---

## Links:

[1] <http://www.sc.edu>

[2] <http://www.privacyrights.org>

[3] <http://www.msnbc.msn.com/id/12322162/>

# San Diego Man Charged with Accessing University Applicants' Information

## Quick Facts

- Date: 4/21/2006
- Institution: [University of Southern California](#) [1]
- Type of Incident: Penetration
- Number Affected: 275,000
- Source: [InfoSec News](#) [2]
- Abstract Source: [North County Times](#) [3]

## Abstract

Eric McCarty, 25-year-old from San Diego, is charged with breaking into the online application system of the University of Southern California. This system contains the Social Security numbers and dates of birth of over 275,000 prospective students that applied to USC between 1997-present. McCarty, who works as a penetration tester and network administrator, allegedly exploited a vulnerability in the application system's database to gain access.

---

## Links:

[1] <http://www.usc.edu>

[2] <http://www.infosecnews.org>

[3] [http://www.nctimes.com/articles/2006/04/21/news/sandiego/17\\_01\\_084\\_20\\_06.txt](http://www.nctimes.com/articles/2006/04/21/news/sandiego/17_01_084_20_06.txt)

## Hackers Get Into UAF Database

### Quick Facts

- Date: 4/21/2006
- Institution: University of Alaska, Fairbanks [1]
- Type of Incident: Penetration
- Number Affected: 39,000
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: Attrition.org [3]

### Abstract

The University of Alaska, Fairbanks suffered a computer breach in one of their server computers that contained the names, Social Security numbers, and partial e-mail address for almost 39,000 current and former students, faculty and staff. The University is not sure if the hacker accessed this information. A security sweep located four other poorly secured server which were taken off line until they could be properly secured.

---

### Links:

[1] <http://www.uaf.edu>

[2] <http://www.privacyrights.org>

[3] <http://attrition.org/dataloss/2006/04/uaf01.html>

# McCombs School of Business Computers Breached

## Quick Facts

- Date: 4/24/2006
- Institution: [University of Texas](#) [1]
- Type of Incident: Unauthorized disclosure
- Number Affected: 197,000
- Source: [InfoSec News](#) [2]
- Abstract Source: [ComputerWorld](#) [3]

## Abstract

A breach of a computer run by the University of Texas' McCombs School of Business exposed 197,000 records of alumni, faculty, staff and current and prospective students. According to the University, some of these records included Social Security Numbers and "possibly other biographical data". The University's attorney general is working with the UT Internet enforcement unit to ensure that affected individuals are notified and protected from possible identity theft.

---

## Links:

[1] <http://www.utexas.edu>

[2] <http://www.infosecnews.org>

[3] <http://www.computerworld.com/securitytopics/security/story/0,10801,110813,00.html>

## Hundreds Affected By Computer Thefts

### Quick Facts

- Date: 4/24/2006
- Institution: University of Virginia [1]
- Type of Incident: Theft
- Number Affected: Hundreds
- Source: Attrition.org [2]
- Abstract Source: The Cavalier Daily [3]

### Abstract

The University of Virginia was the victim of multiple computer thefts recently. A computer stolen from one of UVA's academic buildings contained student information, including Social Security numbers. According to university officials, it appears the thieves were after computer equipment and not the data on the hard drives. However, UVA is urging affected students to closely monitor their credit reports for signs of fraud.

---

### Links:

[1] <http://www.virginia.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.cavalierdaily.com/CVArticle.asp?ID=26961&pid=1440>

# Purdue Warns Graduate Students Over Computer Breach

## Quick Facts

- Date: 4/26/2006
- Institution: Purdue University [1]
- Type of Incident: Penetration
- Number Affected: 1,351
- Source: Privacy Rights Clearinghouse [2]
- Abstract Source: Purdue [3]

## Abstract

Purdue University notified 1,351 current and former graduate students, graduate applicants and a small number of undergraduate that a recent computer breach possible exposed personal information. The compromised computer contained names and Social Security numbers among other information. Purdue has no record that this information was accessed, but cannot rule this possibility out.

---

## Links:

[1] <http://www.purdue.edu>

[2] <http://www.privacyrights.org>

[3] <http://news.uns.purdue.edu/UNS/html3month/2006/060425.Smith.dataincident.html>

# Ohio University Reports Two Separate Security Breaches

## Quick Facts

- Date: 5/2/2006
- Institution: [Ohio University](#) [1]
- Type of Incident: Penetration
- Number Affected: 300,000 (137,000 SSNs)
- Source: [Privacy Rights Clearinghouse](#) [2]
- Abstract Source: [ComputerWorld](#) [3]

## Abstract

Ohio University discovered that a computer thought to have been decommissioned had been compromised as far back as 2005. This breach exposed the names and Social Security numbers of more than 137,000 individuals as well as the personal and biographical information on more than 300,000 individuals and organization at Ohio University. The University is sending out 10,000 e-mails per hour notifying individuals of this breach.

Ohio University was alerted to a second, unknown security breach by the FBI. The FBI became aware of the problem while working on an unspecified case. The server in question housed patent and intellectual property information owned by Ohio University.

---

## Links:

[1] <http://www.ohio.edu>

[2] <http://www.privacyrights.org>

[3] <http://www.computerworld.com/databasetopics/data/story/0,10801,111113,00.html>

# OU's Hudson Health Center Suffers Computer System Breach

## Quick Facts

- Date: 5/12/2006
- Institution: [Ohio University](#) [1]
- Type of Incident: Penetration
- Number Affected: 60,000
- Source: [InfoSec News](#) [2]
- Abstract Source: [Ohio.com](#) [3]

## Abstract

For the third time in as many weeks, Ohio University discovered another breach in its computer systems. This time the computer was part of Ohio University's Hudson Health Center. The names, dates of birth, Social Security numbers and medical information on 60,000 current and former students as well as any faculty or staff who sought treatment at the health center were exposed. Ohio University has launched a complete review of all information systems owned by the university.

---

## Links:

[1] <http://www.ohio.edu>

[2] <http://www.infosecnews.org>

[3] <http://www.ohio.com/mld/beaconjournal/14554413.htm>

# Breach of Public Safety Computer Exposes More Than Social Security Numbers

## Quick Facts

- Date: 5/23/2006
- Institution: [University of Delaware](#) [1]
- Type of Incident: Penetration
- Number Affected: 1,076
- Source: [Attrition.org](#) [2]
- Abstract Source: [University of Delaware UDaily](#) [3]

## Abstract

The University of Delaware is alerting over 1,000 students that a recent breach of a UD Public Safety computer exposed personal information including names, Social Security numbers, and Drivers License numbers. According to university officials it appears this individuals was after the student information on this server and was able to copy some of the information. Officials were quick to point out that university employees quickly enacted the university's incident response plan once the breach was identified. In addition to sending out letters, the university has setup a web site (<http://www.udel.edu/security/identitytheft.html> [4]) to help answer any questions that students may have.

---

## Links:

[1] <http://www.udel.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.udel.edu/PR/UDaily/2006/may/breach052306.html>

[4] <http://www.udel.edu/security/identitytheft.html>

## Google Cache Indexes CSU Stanislaus Student Information

### Quick Facts

- Date: 5/26/2006
- Institution: California State University, Stanislaus [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 1,294
- Source: Attrition.org [2]
- Abstract Source: CSU Stanislaus Newsline [3]

### Abstract

CSU Stanislaus is alerting 1,294 students that their personal information might have been exposed after a file containing student names, addresses, employer information and Social Security numbers was discovered to be available in Google's cache. The file in question was initially leaked to the Google search engine in October 2005 but was quickly removed from both the CSU server and Google's search index. However, it appears that the file remained accessible to all through Google's Google Cache. CSU Stanislaus is currently working with the affected students, offering them one year of free credit monitoring with Equifax.

---

### Links:

[1] <http://www.csustan.edu>

[2] <http://www.attrition.org/dataloss>

[3]

<http://www.csustandur.com/newsline/index.php3?pid=734&action=detail&table=press>

# Computer Breach Exposes Over 130,000 Student Records

## Quick Facts

- Date: 5/26/2006
- Institution: Sacred Heart University [1]
- Type of Incident: Penetration
- Number Affected: 135,000
- Source: Security News Portal [2]
- Abstract Source: ZDNet UK [3]

## Abstract

An attacker was able to breach the computer systems of Sacred Heart University earlier this month. Although little is known about the breach, the university notified 135,000 individuals that their personal information might have been compromised. The information exposed includes Social Security numbers, names, address, and other personal information. Attempts to speak with university officials concerning the breach have been unsuccessful.

---

## Links:

[1] <http://www.sacredheart.edu>

[2] <http://www.snpx.com>

[3] <http://news.zdnet.co.uk/internet/security/0,39020375,39271295,00.htm>

# FIU Student Records Compromised By Hacker

## Quick Facts

- Date: 5/31/2006
- Institution: Florida International University [1]
- Type of Incident: Penetration
- Number Affected: Unknown
- Source: InfoSec News [2]
- Abstract Source: CBS4, Miami, FL [3]

## Abstract

Florida International University sent out notice "postcards" to students alerting the students to a computer breach that occurred two months ago. According to the University a hacker was able to compromise a database containing the names and Social Security numbers of FIU students and applicants. FIU officials have yet to comment about the delay in notification, which has caused worry among the affected students.

---

## Links:

[1] <http://www.fiu.edu>

[2] <http://www.infosecnews.org>

[3] [http://cbs4.com/topstories/local\\_story\\_150225136.html](http://cbs4.com/topstories/local_story_150225136.html)

## Current and Past University of Kentucky Employee Data Exposed Online

### Quick Facts

- Date: 6/1/2006
- Institution: [University of Kentucky](http://www.uky.edu) [1]
- Type of Incident: Unauthorized disclosure
- Number Affected: 1,300
- Source: [Attrition.Org](http://www.attrition.org) [2]
- Abstract Source: [Kentucky.com](http://www.kentucky.com) [3]

### Abstract

The University of Kentucky sent out a memo to over 1,300 current and past employees about the possibility of unintended information exposure. It seems that a spreadsheet containing employee information, including Social Security numbers, was accessible via the Internet. Once UK was notified of this issue, the file was removed immediately. The University of Kentucky does not believe that this information was accessed by any unauthorized individuals but is urging the employees to closely monitor their financial statements for unexpected behavior. The university is in the process of implementing a new computer system to help reduce the chance of a repeat occurrence.

---

### Links:

[1] <http://www.uky.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.kentucky.com/mld/heraldleader/14717374.htm>

## Misplaced Equipment Contains Student Information

### Quick Facts

- Date: 6/1/2006
- Institution: [Miami University](http://www.miami.edu) [1]
- Type of Incident: Loss
- Number Affected: 851
- Source: [Attrition.Org](http://www.attrition.org) [2]
- Abstract Source: [Cleveland.com](http://www.cleveland.com) [3]

### Abstract

A Miami University employee has lost a hand-held computer containing personal information on 851 students. The exact nature of the information exposed was not released. However, the students who enrolled between July 2001 and May 2006 were affected. The University does not believe this information is being used for any illicit activities. However, Miami University has created a program to tighten security controls and increase employee training.

---

### Links:

[1] <http://www.miami.edu>

[2] <http://www.attrition.org/dataloss>

[3]

<http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/1149150686240780.xml&coll=2>

## Social Security Numbers Exposed over Election Dispute

### Quick Facts

- Date: 6/6/2006
- Institution: University of Texas, El Paso [1]
- Type of Incident: Penetration
- Number Affected: 4,719
- Source: Attrition.Org [2]
- Abstract Source: KFoxTv, El Paso, TX [3]

### Abstract

A group of eight to twelve University of Texas, El Paso students illegally gained access to a school computer that contained 4,719 student and faculty Social Security numbers. These students were attempting to find evidence of that a recent Student Government Association (SGA) election was rigged. According to school officials this system contained information pertaining to the 2002 SGA and faculty elections. According to the University, it does not appear that this group of students were trying to do anything illegal with these Social Security numbers. The university is still investigating this incident.

---

### Links:

[1] <http://www.utep.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.kfoxtv.com/news/9332307/detail.html>

## More Computer Breaches Discovered at Ohio University

### Quick Facts

- Date: 6/9/2006
- Institution: [Ohio University](#) [1]
- Type of Incident: Penetration
- Number Affected: 70,000
- Source: [Attrition.Org](#) [2]
- Abstract Source: [Ohio News Now](#) [3]

### Abstract

Ohio University officials announced that two more computer systems were discovered to have been the victims of criminal computer attacks. These recent breaches exposed personal information on over 70,000 individuals including subcontractors paid by Ohio University over the past two years. In a letter sent out to affected individuals the university was quick to point out that there has been no evidence that personal information was being used to commit fraud or identity theft.

---

### Links:

[1] <http://www.ohio.edu>

[2] <http://www.attrition.org/dataloss>

[3]

<http://www.onnnews.com/?sec=home&story=10tv/content/pool/200606/1770514625.htm>

1

## Western Illinois University Security Breach Exposes 240,000 Records

### Quick Facts

- Date: 6/17/2006
- Institution: Western Illinois University [1]
- Type of Incident: Penetration
- Number Affected: 240,000
- Source: Attrition.Org [2]
- Abstract Source: Belleville News Democrat [3]

### Abstract

A computer containing the names, address and Social Security numbers of 240,000 people connected to Western Illinois University was breached on June 5, 2006. The university was aware of the incident as soon as it occurred and took immediate steps to correct the vulnerability. Since the intruder only had access for a short amount of time, the university is not aware of any records that were viewed or copied.

---

### Links:

[1] <http://www.wiu.edu>

[2] <http://www.attition.org/dataloss>

[3] <http://www.belleville.com/mld/belleville/news/state/14843503.htm>

# University Kidney Transplant Program Computer Stolen

## Quick Facts

- Date: 6/20/2006
- Institution: University of Alabama, Birmingham [1]
- Type of Incident: Theft
- Number Affected: 9,800
- Source: Attrition.Org [2]
- Abstract Source: Attrition.org [3]

## Abstract

A laptop belonging to the University of Alabama, Birmingham's kidney transplant program containing donor, recipient and potential recipient information has been stolen. This computer was taken from a locked office back in February, but the university delayed notifications until it could reconstruct all of the missing data. According to university officials, the information on this computer included names, Social Security numbers, and medical information of the 9,800 individuals involved in the transplant program.

A university spokesperson mentioned that there is no evidence that this information has been used for any illegal purposes and that the university has increased physical security measures. However, the University of Alabama is offering one year of free credit monitoring to all affected individuals.

---

## Links:

[1] <http://www.uab.edu>

[2] <http://attrition.org/dataloss>

[3] <http://attrition.org/dataloss/2006/06/uab01.html>

## Stolen USB Drive Contained 18 Years of Student Information

### Quick Facts

- Date: 6/22/2006
- Institution: [University of Kentucky](http://www.uky.edu) [1]
- Type of Incident: Theft
- Number Affected: 6,500
- Source: [Attrition.org](http://www.attrition.org) [2]
- Abstract Source: [The Kentucky Kernel](http://www.kykernel.com) [3]

### Abstract

The University of Kentucky is alerting 6,500 students that their personal information is at risk after the recent theft of a USB flash drive containing class rosters from a classroom. UK estimates this 4GB drive contained up to 130 files containing UK School of Human and Environmental Sciences class rosters dating from 1988 to 2006. These rosters contained student names, grades and Social Security numbers, which UK uses as student IDs. The university is currently phasing out the use of SSNs as student IDs, a plan that will be complete by October.

---

### Links:

[1] <http://www.uky.edu>

[2] <http://www.attrition.org/dataloss>

[3]

<http://www.kykernel.com/media/storage/paper305/news/2006/06/22/CampusNews/Current.And.Former.Students.At.Risk.For.Identity.Theft-2118127.shtml?norewrite200612171404&sourcedomain=www.kykernel.com>

## Laptop Containing 3,000 SFSU Student Records Stolen

### Quick Facts

- Date: 6/23/2006
- Institution: [San Francisco State](#) [1]
- Type of Incident: Theft
- Number Affected: 3,000
- Source: [Attrition.Org](#) [2]
- Abstract Source: [SFGate.com](#) [3]

### Abstract

San Francisco State University (SFSU) has announced that a laptop has been stolen from the car of a faculty member. This laptop contained about 3,000 names and Social Security numbers belonging to current and former SFSU students. Grades and telephone numbers of some students were also on this laptop. While the laptop was stolen on June 1, the university was not notified of the incident until June 6. According to a university spokesperson, the university has taken appropriate action, but it is not uncommon for faculty to keep student information on their computers. The spokesperson declined to answer questions about disciplinary action. Police are investigating this as a typical car break-in and do not believe the thief knew about the data contained on the laptop.

---

### Links:

[1] <http://www.sfsu.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/06/23/BAGQLJJ2LB1.DTL>

# University of Tennessee Suffers Computer breach

## Quick Facts

- Date: 7/6/2006
- Institution: University of Tennessee [1]
- Type of Incident: Penetration
- Number Affected: 36,000
- Source: Attrition.org [2]
- Abstract Source: WBIR, Knoxville, TN [3]

## Abstract

For nine months (Aug 05 - May 06) a computer hacker illegally accessed a University of Tennessee computer that contained employee information. This information included names, address and Social Security numbers of around 36,000 current and former UT employees. It appears that this hacker used the computer to store and transmit motion pictures and UT officials do not believe the employee information was used accessed. The University of Tennessee has setup a toll-free number for any current or former employee that might have questions about the breach. That number is 866-748-1680.

---

## Links:

[1] <http://www.utk.edu>

[2] <http://attrition.org/dataloss>

[3] <http://www.wbir.com/news/local/story.aspx?storyid=35838&provider=kns>

## Stolen Laptop Stolen Contains U of I Student SSNs

### Quick Facts

- Date: 7/14/2006
- Institution: [University of Iowa](#) [1]
- Type of Incident: Theft
- Number Affected: 280
- Source: [Attrition.org](#) [2]
- Abstract Source: [The Des Moines Register](#) [3]

### Abstract

The University of Iowa is reducing the use of student Social Security numbers after the theft of a laptop containing information on 280 students. The laptop in question belonged to a MBA professor and was stolen from the professor's office in Davenport, IA. Information contained on this laptop included personal information including Social Security numbers and some contact information for 280 former and current U of I MBA students. The University does not believe that this information has been used and quoted a police statement that in most cases the thieves wipe the hard drives before using the stolen laptops.

---

### Links:

[1] <http://www.uiowa.edu>

[2] <http://www.attrition.org/dataloss>

[3]

<http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20060714/NEWS02/607140380>

## Data Breach Occurs at Northwestern

### Quick Facts

- Date: 7/14/2006
- Institution: Northwestern University [1]
- Type of Incident: Penetration
- Number Affected: 17,000
- Source: Attrition.org [2]
- Abstract Source: Northwestern [3]

### Abstract

An unauthorized person not affiliated with Northwestern University illegally accessed nine desktop computers belonging to the Office of Admissions and Financial Aid. These nine computers contained names and personal information, including some Social Security numbers, on as many as 17,000 individuals. Northwestern officials are urging any students who provided Social Security number information to the Office of Admissions and Financial Aid to follow the FTC's identity theft precaution instructions. However, the University does not believe that the unauthorized individual accessed or was even aware of the student information on these computers.

---

### Links:

[1] <http://www.northwestern.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.northwestern.edu/newscenter/stories/2006/07/data.html>

## E-Health Trial Puts Patient Data At Risk

### Quick Facts

- Date: 7/25/2006
- Institution: [Georgetown University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 5,600 to 23,000
- Source: [Attrition.org](#) [2]
- Abstract Source: [Wired](#) [3]

### Abstract

A trial run of an electronic prescription-writing program ends in the accidental exposure of 5,600 to 23,000 Georgetown University Hospital patient data. The patient information was exposed online due to a hard-coded database password. While no medial data was exposed, names, addresses, Social Security numbers, and dates of birth were available. This flaw in the online system was discovered by a computer consultant while working to install the medical software, InstantDx, for a client. There is no evidence that any unauthorized individuals had access the Georgetown University Hospital information but the Hospital has suspended the trail program.

InstantDX was quick to accept responsibility and has since secured its systems. The company chairman and CEO Allan Weinstein calls the incident "a one-time quirk."

---

### Links:

[1] <http://www.georgetown.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.wired.com/news/technology/0,71453-0.html>

## Security Breach Affects Patrons of the Arts and Doctoral Candidates Alike

### Quick Facts

- Date: 08/01/2006
- Institution: [Wichita State University](#) [1]
- Type of Incident: Penetration
- Number Affected: 2,040
- Source: [Attrition.org](#) [2]
- Abstract Source: [The Wichita Eagle](#) [3]

### Abstract

An unknown individuals breached three of the computers in Wichita State University's College of Fine Arts box office and a server belonging to the psychology department. The box office computers contained credit card information on 2,000 individuals while the psychology server contained data on 40 doctoral program applicants. The University has no evidence that any information exposed during these breaches has been used for Identity Theft. However, the University has sent out notifications to all affected individuals and WSU has alerted the three major US credit bureaus. Wichita State University has taken immediate action to secure the affected computer and is investigating the apparent lack of security.

---

### Links:

[1] <http://www.wichita.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.kansas.com/mld/kansas/15174146.htm>

## Stolen Laptop Contained Social Security Numbers on 3,020 Physics and Astronomy Students

### Quick Facts

- Date: 08/01/2006
- Institution: [California Polytechnic State University](http://www.calpoly.edu) [1]
- Type of Incident: Theft
- Number Affected: 3,020
- Source: [Attrition.org](http://www.attrition.org) [2]
- Abstract Source: [San Luis Obispo Tribune](http://www.sanluisobispo.com/mld/sanluisobispo/news/15169992.htm) [3]

### Abstract

A laptop stolen from the home of Cal Poly professor John Mottman contained the Social Security numbers on any student that took Mottman's astronomy or physics lectures between 1994 and 2004. During this period, Cal Poly used Social Security numbers on class lists as unique identifiers. This practice ended in 2004. In fact, Cal Poly is attempting to change its practice of using Social Security numbers altogether. Cal Poly is recommending that any affected student contact one of the three major credit bureaus and request a fraud alert be placed on their credit report.

---

### Links:

[1] <http://www.calpoly.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.sanluisobispo.com/mld/sanluisobispo/news/15169992.htm>

# Stolen Laptop Contains Employee Information

## Quick Facts

- Date: 08/02/2006
- Institution: [Belhaven College](#) [1]
- Type of Incident: Theft
- Number Affected: Up to 300
- Source: [Attrition.org](#) [2]
- Abstract Source: [The Clarion Ledger](#) [3]

## Abstract

A Belhaven College employee was approached from behind in a Belhaven parking lot and robbed of their wallet and a laptop computer which contained Social Security numbers, names and bank account information on a number of Belhaven employees. While the College is not aware of how many employees are affected, Belhaven issued a memo to all employees warning of the possibility of Identity Theft. According to Belhaven College President Roger Parrott, there have been no reported ID thefts related to this theft and the memo was sent out as a precaution. In this memo Parrott suggests that employees contact one of the three major credit bureaus and alert them to the possibility of Identity Theft.

---

## Links:

[1] <http://www.belhaven.edu>

[2] <http://www.attrition.org/dataloss>

[3]

<http://www.clarionledger.com/apps/pbcs.dll/article?AID=/20060802/NEWS/608020375>

## Kentucky Discovers Two Incidents On The Same Day

### Quick Facts

- Date: 08/15/2006
- Institution: [University of Kentucky](#) [1]
- Type of Incident: Unauthorized disclosure
- Number Affected: 710
- Source: [Attrition.org](#) [2]
- Abstract Source: [WKYT Kentucky \(Attrition.org Archive\)](#) [3]

### Abstract

Student information, including Social Security numbers, was accidentally posted to a University of Kentucky e-mail list. This information, a list of 630 students receiving financial aid information, contained student names and SSNs, which UK still uses as student ID numbers. UK has a plan in place already to stop using Social Security numbers in October of this year. Jay Blanton, a PR specialist for the University, calls the mistake regrettable and says students have been notified.

On this same day, UK discovered an incident at the University's Department of Geography that involved personal information on 80 students.

---

### Links:

[1] <http://www.uky.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://attrition.org/dataloss/2006/08/uk01.html>

## Rogue WiFi APs Put Data At Risk

### Quick Facts

- Date: 8/25/2006
- Institution: [University of Iowa](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: Unknown
- Source: [InfoSec News](#) [2]
- Abstract Source: [The Des Moines Register](#) [3]

### Abstract

A recent audit of wireless connectivity at the University of Iowa uncovered 80 rogue access points (APs) throughout nine academic buildings. Over half of these APs had no encryption or security features enabled, leaving both the U of I network and student information vulnerable to attack. It is believed that impatience caused faculty and staff installed these wireless access points. Current wireless access only covers about 15% of the U of I campus. The University of Iowa is currently working on pinpointing these rogue access points and converting these APs either to authorized access points (with security features enabled) or back to wired connections. U of I is also working towards expanding its overall wireless coverage.

---

### Links:

[1] <http://www.uiowa.edu>

[2] <http://www.infosecnews.org>

[3]

<http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20060824/NEWS02/608240380/1001/NEWS>

# Unauthorized Computer Access Uncovered During USC Audit

## Quick Facts

- Date: 8/26/2006
- Institution: University of South Carolina [1]
- Type of Incident: Penetration
- Number Affected: 6,000
- Source: Attrition.org [2]
- Abstract Source: The State (via Attrition mirror) [3]

## Abstract

The University of South Carolina recently warned 6,000 students that their personal information is a risk due to a computer breach. A recent computer security audit revealed that an unknown individual gained unauthorized access to a computer server back in September 2005. This server contained student information including names and Social Security numbers. The university is not aware of any illegal use of this information but expresses regret over the incident. According to officials the incident should have occurred and USC has secured the server.

---

## Links:

[1] <http://www.sc.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://attrition.org/dataloss/2006/08/usc01.html>

# Google Search Reveals Personal Information

## Quick Facts

- Date: 9/1/2006
- Institution: [Virginia Commonwealth University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 2,100
- Source: [Attrition.org](#) [2]
- Abstract Source: [Times Dispatch](#) [3] via [Attrition.org mirror](#) [4]

## Abstract

A Virginia Commonwealth University student looking up her own name on Google found more than she expected to find. A file from the VCU School of Engineering containing over 2,100 student records was available online, and indexed through the Google search engine. Contained in this file were student names, Social Security numbers and e-mail address. According to VCU officials, this file was left online due to human error and it is working toward ensuring the safety of all student information. VCU has put up a website for any student that has concerns.

---

## Links:

- [1] <http://www.vcu.edu>
- [2] <http://www.attrition.org/dataloss>
- [3] <http://www.timesdispatch.com>
- [4] <http://attrition.org/dataloss/2006/09/vcu01.html>

## Stolen Computers Contain Student Information

### Quick Facts

- Date: 09/08/2006
- Institution: University of Minnesota [1]
- Type of Incident: Theft
- Number Affected: 13,084 (including 603 Social Security Numbers)
- Source: Attrition.org [2]
- Abstract Source: St. Paul Pioneer Press [3]

### Abstract

Two computers stolen from desk of a program coordinator within University of Minnesota's Institute of Technology contained personal data on over 13,000 students who joined the University between 1992 and 2006. Birth dates, phone numbers, high school information, grades and test scores were some of the data contained on these laptops. Also on these laptops were the Social Security numbers on roughly 600 students. The University sent out letters on August 30th to notify students of the potential risk. While the University no longer uses Social Security numbers as student identifiers, older records did contain this information.

---

### Links:

[1] <http://www.umn.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.twincities.com/mld/pioneerpress/news/local/15475291.htm>

# University Uncovers Unauthorized Access During Routine Risk Assessment

## Quick Facts

- Date: 09/15/2006
- Institution: [University of Texas, San Antonio](#) [1]
- Type of Incident: Penetration
- Number Affected: 64,000
- Source: [Attrition.org](#) [2]
- Abstract Source: [San Antonio Express News](#) [3]

## Abstract

The University of Texas at San Antonio notified 53,000 current and former students and 11,000 faculty and staff notifying these individuals that their personal information might have been exposed due to a computer security breach. However, University officials were quick to point out that this breach was discovered before any information was copied or altered. This breach was discovered during a routine risk assessment of UTSA's computer servers. The breached server contained names, addresses, Social Security numbers, and financial aid information. UTSA's technology team and local police are currently investigating this incident.

---

## Links:

[1] <http://www.utsa.edu>

[2] <http://www.attrition.org/dataloss>

[3]

<http://www.mysanantonio.com/news/metro/stories/MYSA091606.02B.UTSAHACKER.2e77063.html>

## Berry College "Misplaces" Social Security Numbers

### Quick Facts

- Date: 09/20/2006
- Institution: [Berry College](#) [1]
- Type of Incident: Loss
- Number Affected: 2,093
- Source: [Attrition.org](#) [2]
- Abstract Source: [Rome News-Tribune](#) [3]

### Abstract

An external financial aid consultant working for Berry College "misplaced" financial aid information on over 2,000 students at a regional airport. This information, both in paper and digital format, included incomes, names and Social Security numbers and other information included on student FAFSA applications. Berry officials did point out that this information does not contain enough detail for identity theft on its own. Missing are birth dates and places and account information. However, Berry has setup a hotline for students and parents with questions and/or concerns.

---

### Links:

[1] <http://www.berry.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://news.mywebpal.com/partners/680/public/news748399.html>

## "Identity Issues Are Definitely At Risk" After Laptop Theft

### Quick Facts

- Date: 09/20/2006
- Institution: University of Wisconsin, Whitewater [1]
- Type of Incident: Theft
- Number Affected: Unknown
- Source: ESI [2]
- Abstract Source: Royal Purple News [3]

### Abstract

Six laptops were among the equipment stolen from the University of Wisconsin, Whitewater's Heide Hall. The theft was discovered by Communications Department Chairperson Wilfred Tremblay. Associate Professor Susan Wildermuth was also a victim of this theft. According to Wildermuth, "All my files related to teaching, research, and letters of recommendation were stolen, and identity issues are definitely at risk as well." It is not known how many students are affected by this theft or what, if any, personal information was exposed. UWW campus police consider this theft to be an open-pending investigation.

---

### Links:

[1] <http://www.uww.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.royalpurplenews.com/disarticle.php?id=1656&dateid=2006-09-20>

## Computers Missing From Storage Contained Student Information

### Quick Facts

- Date: 09/22/2006
- Institution: University of Colorado, Boulder [1]
- Type of Incident: Loss
- Number Affected: 1,372
- Source: Attrition.org [2]
- Abstract Source: University of Colorado at Boulder [3]

### Abstract

Two computers containing student information were discovered to be missing from the University of Colorado at Boulder's Leeds School of Business. These computers were placed in storage last May. The loss was discovered when the Leeds staff removed these computers at the end of August in preparation for the new school year. Social Security numbers, names, and grades were amount the information contained on these laptops. Although the CU-Boulder officials do not believe any personal information has been accessed, the University has notified the 1,372 affected students and setup both a web site and hotline for student that might have questions or concerns over this loss.

---

### Links:

[1] <http://www.colorado.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.colorado.edu/news/releases/2006/308.html>

## Purdue Notifies Alumni of Computer Breach

### Quick Facts

- Date: 09/22/2006
- Institution: [Purdue University](#) [1]
- Type of Incident: Penetration
- Number Affected: 2,500
- Source: [InfoSec News](#) [2]
- Abstract Source: [FortWayne.com](#) [3]

### Abstract

Purdue University notified individuals who attend the university in 2000 about a recently discovered security breach. 2,500 alumni were told that their personal information, including Social Security numbers and names, may have been accessed by an unauthorized individual. Purdue officials discovered that a workstation in the chemistry department might have been accessed by an unauthorized individual who installed remote access software on the computer. This computer was found to contain a Feb 2000 files that contained former student information.

---

### Links:

[1] <http://www.purdue.edu>

[2] <http://www.infosecnews.org/>

[3] <http://www.fortwayne.com/mld/newssentinel/news/local/15585500.htm>

## Multiple Laptop Theft Exposes Patient Data

### Quick Facts

- Date: 09/24/2006
- Institution: Nagasaki University [1]
- Type of Incident: Theft
- Number Affected: 9,000
- Source: Attrition.org [2]
- Abstract Source: The Daily Yomiuri [3]

### Abstract

Six laptop computers contain information on 9,000 patients were stolen from Nagasaki University's Hospital of Medicine and Dentistry. Information contained on these laptops includes names, genders, birth dates, and diagnoses of the hospital's hematology division. These laptops were stolen from a Hospital laboratory. According to university officials passwords had only been set on 2,000 of the records on the laptops. The hospital alerted police as soon as the theft was discovered and officials for the university apologized for the security breach and exposure.

---

### Links:

[1] <http://www.nagasaki-u.ac.jp/english/>

[2] <http://attrition.org/dataloss>

[3] <http://www.yomiuri.co.jp/dy/national/20060924TDY02007.htm>

## Student Notified About Breach at a Different University

### Quick Facts

- Date: 09/27/2006
- Institution: Sacred Heart University [1]
- Type of Incident: Penetration
- Number Affected: Unknown
- Source: ESI [2]
- Abstract Source: NBC30, Connecticut [3]

### Abstract

Stacey Koblinski, a recent college graduate, received a notification from Sacred Heart University that her personal information may have been exposed during a recent computer breach. Making matters worse, Ms. Koblinski was never a student at Sacred Heart University. It seems that Sacred Heart is one of a large number of colleges and universities that purchase student information from testing agencies. Many of these testing agencies still use Social Security numbers as student identifiers. However, ACT and SAT are phasing out the use of student SSNs on standardized tests. Sacred Heart University is still investigating the breach.

---

### Links:

[1] <http://www.sacredheart.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.nbc30.com/news/9949938/detail.html>

# University Research Information Exposes Participant Data

## Quick Facts

- Date: 09/29/2006
- Institution: University of Iowa [1]
- Type of Incident: Penetration
- Number Affected: 14,500
- Source: ESI [2]
- Abstract Source: Iowa City Press-Citizen [3]

## Abstract

The University of Iowa has discovered that a computer used in a study on maternal and child health going back to 1995 was breached by computer attackers. Among other things, this computer contained the Social Security numbers on the 14,500 individuals that have participated in this study of the years. UI has sent out a letter to all affected individuals with instructions on how to monitor credit reports and place fraud alerts with the major credit agencies. University officials believe the attack to be the work of individuals seeking a place to store video files for illegal distribution. However, the university has contacted law enforcement and an investigation has been launched.

---

## Links:

[1] <http://www.uiowa.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.press-citizen.com/apps/pbcs.dll/article?AID=/20060929/NEWS01/60929003/1079>

## Stolen Laptop Contains Information on Aspiring High School Students

### Quick Facts

- Date: 10/11/2006
- Institution: [Adams State College](#) [1]
- Type of Incident: Theft
- Number Affected: 184
- Source: [Attrition.org](#) [2]
- Abstract Source: [Valley Courier Online](#) [3]

### Abstract

A laptop containing personal information on 184 high school students was stolen from locked closet at Adams State College. This laptop was part of college's Upward Bound program, which aims to help first-generation, low income high school students improve their potential college success. The college has notified all of the students affected by this theft and advised these students of the steps they should take to prevent identity theft. Adams officials did state that personal student information is no longer kept on personal computers. Adams State College Public Safety office has setup a phone line for anyone with questions about this incident.

---

### Links:

[1] <http://www.adams.edu>

[2] <http://www.attrition.org>

[3] [http://www.alamosanews.com/main.php?story\\_id=13586&page=39](http://www.alamosanews.com/main.php?story_id=13586&page=39)

# Donor Information Stolen During Computer Breach

## Quick Facts

- Date: 10/12/2006
- Institution: Brock University [1]
- Type of Incident: Penetration
- Number Affected: 70,000
- Source: ESI [2]
- Abstract Source: CBC News [3]

## Abstract

Personal information on 70,000 Brock University donors was stolen from a university computer during recent computer breach on September 22. Included in this information was about 90 credit cards and information on 270 bank accounts. This intruder used "secret passwords" to gain access to information on every Brock University donor according to Terry Boak, Brock's Vice President. Boak also said this intruder went straight for the donor information. The intruder was in and out in four minutes. While these individuals were notified by the university, Brock University did not see any "value" in releasing this information to the public.

---

## Links:

[1] <http://www.brocku.ca>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.cbc.ca/technology/story/2006/10/12/tech-brock.html>

## Yet Again, Stolen Computers Contain Student Information

### Quick Facts

- Date: 10/12/2006
- Institution: University of Texas, Austin [1]
- Type of Incident: Theft
- Number Affected: 2,500
- Source: Attrition.org [2]
- Abstract Source: The Houston Chronicle [3]

### Abstract

The University of Texas at Austin alerted 2,500 students that their personal information, including Social Security numbers, were contained on two computers stolen from faculty members home on September 29. The affected student are those that took computer science or engineering classes from Ray Springston between fall 2005 and fall 2006. The school is providing students information on how to monitor their credit reports for suspicious activity and has setup a web site to assist affected students. The Fort Worth police are currently investigating this theft, but currently have no leads.

---

### Links:

[1] <http://www.utexas.edu>

[2] <http://www.attrition.org>

[3] <http://www.chron.com/disp/story.mpl/metropolitan/4253257.html>

## Bad Day for U of M, Part 1

### Quick Facts

- Date: 10/20/2006
- Institution: University of Minnesota [1]
- Type of Incident: Theft
- Number Affected: 13,000
- Source: ESI [2]
- Abstract Source: The Pioneer Press [3]

### Abstract

University of Minnesota officials announced on Thursday the theft of two university laptops in August. The stolen laptops belonged to U of M's Institute of Technology and contained personal information on more the 13,000 U of M students. Social Security numbers were among the personal student data on these two laptops. While the laptops in question did contain encryption software, university officials report difficulty in getting professors and staff member to use this software.

---

### Links:

[1] <http://www.umn.edu>

[2] <http://www.adamdodge.com>

[3] <http://www.twincities.com/mld/twincities/news/state/minnesota/15807799.htm>

## Bad Day for U of M, Part 2

### Quick Facts

- Date: 10/20/2006
- Institution: University of Minnesota [1]
- Type of Incident: Theft
- Number Affected: 200
- Source: ESI [2]
- Abstract Source: The Pioneer Press [3]

### Abstract

Hot on the heels of the university's Institute of Technology laptop theft announcement, University of Minnesota officials announce yet another laptop theft. This laptop was stolen from an art department faculty member in June during this individuals trip to Spain. While the laptop contained student information such as names, student IDs and grades, no Social Security numbers were exposed. University officials say that the university is in the process of training faculty and staff on the importance of information security.

---

### Links:

[1] <http://www.umn.edu>

[2] <http://www.adamdodge.com>

[3] <http://www.twincities.com/mld/twincities/living/15801934.htm>

## College Notifies Students and Staff Over Failed Intrusion Attempt

### Quick Facts

- Date: 10/28/2006
- Institution: St. Norbert College [1]
- Type of Incident: Penetration
- Number Affected: unknown
- Source: ESI [2]
- Abstract Source: Green Bay Press-Gazette [3]

### Abstract

St. Norbert College announced an attempted attack on one of the college's computer systems occurred earlier this month. The breach was uncovered when a college employee received complaints about computer performance and began investigating the problem. What the director of computer services discovered was an attempted intrusion on one of the systems and a mysterious software package. According to a college spokesperson they intrusion failed and no data was exposed. However, St. Norbert College notified all students, faculty and staff about the attempt and to notify the college if they notice any unusual behavior. The college has notified local law enforcement and is attempting to be as proactive as possible to help protect the college as well as students and employees.

---

### Links:

[1] <http://www.snc.edu>

[2] <http://www.adamdodge.com/esi>

[3]

<http://www.greenbaypressgazette.com/apps/pbcs.dll/article?AID=/20061028/GPG0101/610280518/1207/GPGnews>

## University Assists Master's Student Even Though Breach Did Not Affect University Systems

### Quick Facts

- Date: 10/29/2006
- Institution: [Nanyang Technological University](#) [1]
- Type of Incident: Penetration
- Number Affected: 1
- Source: [ESI](#) [2]
- Abstract Source: [The Electric New Paper, Singapore](#) [3]

### Abstract

First-year master's student, Susaria Srinivas, suffers two security attacks that destroy three years worth of work. These breaches occurred on Srinivas personal laptop while he was connect to the Nanyang Technological University network. NTU quickly responded when Srinivas' reported the breaches but staff members found no problems with university systems. In addition, the university has received no other reports from students, faculty or staff about computer problems. However, NTU personnel did take the initiative to help Srinivas update his out-of-date anti-virus software as well as help him figure out what happened to his computer. It appears that an unknown individual gained access to Srinivas' computer and installed two remote control trojan horse programs on the laptop.

---

### Links:

[1] <http://www.ntu.edu.sg/>

[2] <http://www.adamdodge.com/esi>

[3] <http://newpaper.asia1.com.sg/news/story/0,4136,116402,00.html>

## Villanova Latest Institution Affected By Laptop Theft

- Date: 11/02/2006
- Institution: Villanova University [1]
- Type of Incident: Theft
- Number Affected: 1,243
- Source: ESI [2]
- Abstract Source: CentreDaily.com [3]

### Abstract

A stolen laptop belonging to an insurance brokerage firm contained personal information on over 1,200 Villanova students. Students names, dates of birth and driver's license numbers were among the data contained on this laptop. Affected students will receive free credit monitoring services from Villanova, according to university officials. The university notified those affected in an Oct 26 letter. However, a story in the Villanovan [4], Villanova's student newspaper, condemns the university for notifying parents of affected students instead of the students themselves.

---

### Links:

[1] <http://www.villanova.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.centredaily.com/mld/centredaily/news/politics/15913680.htm>

[4]

<http://www.villanovan.com/media/storage/paper581/news/2006/11/02/Opinion/University.Should.Adopt.Tough.Love-2414460.shtml?norewrite200611021934&sourcedomain=www.villanovan.com>

## University Delays Notifying Students of SSN E-mail Mix-up

### Quick Facts

- Date: 11/03/2006
- Institution: [University of Virginia](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 632
- Source: [Attrition.org](#) [2]
- Abstract Source: [The Cavalier Daily](#) [3]

### Abstract

The University of Virginia's Student Financial Services accidentally e-mailed student names and Social Security numbers to wrong students. Instead of 1,264 e-mail alerts, SFS sent out 632 e-mails to students, the problem is that these e-mails contained the names and SSNs of the 632 students who did not receive any e-mail. While university officials say staff member immediately began correcting the computer program responsible for the leak, it has yet to send out any notification to affected students. One student, Will Rucker, did not know anything was amiss until The Cavalier Daily contacted him about the problem. UVA officials say the university will be notifying students of the error soon.

---

### Links:

[1] <http://www.virginia.edu>

[2] <http://attrition.org/dataloss>

[3] <http://www.cavalierdaily.com/CVArticle.asp?ID=28435&pid=1507>

# Laptop Containing Student Information Stolen and Recovered

## Quick Facts

- Date: 11/14/2006
- Institution: Connors State College [1]
- Type of Incident: Theft
- Number Affected: 22,500
- Source: ESI [2]
- Abstract Source: KTEN.com [3]

## Abstract

Connors State College officials just announced the theft and recovery of a college laptop that contained information the thousands of students involved in the Oklahoma Higher Learning Access Program (OHLAP) scholarship. All told, the names, address and Social Security numbers on 22,500 students were contained on this laptop. A current Connors student is under investigation for the theft. According to school officials, there is no evidence that this information was accessed, but Connors is encouraging all students affected to closely monitor their credit statements.

---

## Links:

[1] <http://www.connors.cc.ok.us>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.kten.com/Global/story.asp?S=5679797>

## E-mail "Not Intended For [Student] Review" Exposes Social Security Numbers

### Quick Facts

- Date: 11/17/2006
- Institution: [Jefferson College of Health Sciences](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 143
- Source: [Attrition.org](#) [2]
- Abstract Source: [WSLS, News Channel 10](#) [3]

### Abstract

An e-mail sent by Jefferson College of Health Sciences (JCHS) financial aid director accidentally exposes 143 student names and social security numbers. According to the college, the e-mail was intended for another college employee but ended up being sent every one of JCHS's 900 students. An e-mail from Carol Seavor, the college president, urged students to immediately delete this e-mail since "the information was not intended for [student] review." JCHS is also willing to pay for one year of credit monitoring for all affected students.

---

### Links:

[1] <http://www.jchs.edu>

[2] <http://www.attrition.org/dataloss>

[3]

[http://www.wsls.com/servlet/Satellite?pagename=WSLS%2FMGArticle%2FSLS\\_BasicArticle&c=MGArticle&cid=1149191744743&path=!news!localnews](http://www.wsls.com/servlet/Satellite?pagename=WSLS%2FMGArticle%2FSLS_BasicArticle&c=MGArticle&cid=1149191744743&path=!news!localnews)

## Thief Makes Off With Years Of Research Data

### Quick Facts

- Date: 11/23/2006
- Institution: University of Colorado, Boulder [1]
- Type of Incident: Theft
- Number Affected: N/A
- Source: ESI [2]
- Abstract Source: CBS 4, Denver [3]

### Abstract

A thief made off with a University of Colorado computer containing several years worth of graduate research. The computer in question belonged to the university's Engineering Center. According to Engineering faculty, the research is of little use to most people. The University of Colorado and the Boulder County Crime Stoppers are offering a \$1,000 reward to any information leading to an arrest and criminal charges.

---

### Links:

[1] <http://www.colorado.edu>

[2] <http://www.adamdodge.com/esi>

[3] [http://cbs4denver.com/topstories/local\\_story\\_327100741.html](http://cbs4denver.com/topstories/local_story_327100741.html)

## Theft Puts Student, Faculty Identities At Risk

### Quick Facts

- Date: 11/28/2006
- Institution: California State, Los Angeles [1]
- Type of Incident: Theft
- Number Affected: 2,534
- Source: Attrition.org [2]
- Abstract Source: CBS2/KCAL9 [3]

### Abstract

Cal State, L.A. officials recently contacted over 2,500 students, applicants and faculty members and informed these individuals that their identities are at risk. A USB drive containing names, Social Security numbers, campus ID numbers, e-mail address and phone numbers of individuals in the university's teacher credential program was in a purse stolen from a Cal State, L.A. employee's car. According to university officials, it is not known whether or not the thief has accessed this information, but the university is concerned about student identification safety and preventing such an incident from occurring in the future. The university has urged student to contact the major credit bureaus and has also setup a set up a toll-free calling center at (800) 883-4029 and a Web site, [www.calstatela.edu/usbincident](http://www.calstatela.edu/usbincident) [4].

---

### Links:

[1] <http://www.calstatela.edu>

[2] <http://www.attrition.org/dataloss>

[3] [http://cbs2.com/topstories/local\\_story\\_332234121.html](http://cbs2.com/topstories/local_story_332234121.html)

[4] <http://www.calstatela.edu/usbincident>

## Chinese Hack Naval War College

### Quick Facts

- Date: 11/30/2006
- Institution: Naval War College [1]
- Type of Incident: Penetration
- Number Affected: N/A
- Source: ESI [2]
- Abstract Source: The Washington Times [3]

### Abstract

Earlier this month, Chinese hackers penetrated and, according to Retired Air Force Maj. Gen. Richard Goetze, "took down" the Naval War College's computer network. According to a college spokesperson, all affected machines have been disconnected from the network and are undergoing digital forensic investigations to help the Navy determine the specifics of the attack. The FBI and NCIS are also investigating the computer attack. It is unknown at this point if this attack is related to "Titan Rain", the government code-name for the recent increase in cyber-attacks against US military and defense institutions coming from China. Officials declined to comment further on the incident but did state that this was an isolated incident that did not affect any other Department of Defense networks.

---

### Links:

[1] <http://www.nwc.navy.mil>

[2] <http://www.adamdodge.com/esi>

[3] <http://washingtontimes.com/national/20061130-103049-5042r.htm>

## Thieves Make Off With Computers From University Offices

### Quick Facts

- Date: 12/04/2006
- Institution: [Troy University](#) [1]
- Type of Incident: Theft
- Number Affected: Unknown
- Source: [ESI](#) [2]
- Abstract Source: [WSFA 12](#) [3]

### Abstract

Thieves made off with four computers from the Math and Science Hall at Troy University. Three of the computers in question were taken from the office of Dr. Don Jeffery. It appears that there was evidence that these thieves attempted to break into several other offices in the area. The campus is not sure if this was an inside job or not, but is investigating the theft. There is no word on whether or not these computers contained any student or other sensitive university information.

---

### Links:

[1] <http://www.troy.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.wsfa.com/Global/story.asp?S=5767907&nav=0RdE>

## Print Out Containing 21,000 Student Records Stolen

### Quick Facts

- Date: 12/05/2006
- Institution: Nassau Community College [1]
- Type of Incident: Theft
- Number Affected: 21,000
- Source: ESI [2]
- Abstract Source: Newsday [3]

### Abstract

Someone stole a print out containing information on the entire Nassau Community College students body. All told, this print out contained the Social Security numbers, name, address and phone number on more than 21,000 NCC students. According to NCC officials, this list was stolen off the desk of an employee in the NCC Student Activities Office when this employee stepped away for about 10 minutes. NCC is offering one year of free credit monitoring for all student affected by this incident. Nassau County Police, FBI and DHS were all notified of this incident.

---

### Links:

[1] <http://www.ncc.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.newsday.com/news/local/longisland/ny-licoll1205,0,7551763.story?coll=ny-top-headlines>

## E-mail Exposes Personal Student Information

### Quick Facts

- Date: 12/9/2006
- Institution: [Virginia Commonwealth University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 591
- Source: [ESI](#) [2]
- Abstract Source: [The Times Dispatch](#) [3]

### Abstract

Virginia Commonwealth University has begun contacting 591 students to inform them that their personal information was accidentally included in an e-mail sent to 194 VCU students. This e-mail, sent to individuals eligible for the Phi Kappa Phi honor society, included students names, Social Security numbers, permanent addresses and grade point averages. According to university officials, VCU has contracted with an outside firm to provide credit monitoring and identity theft protection for all students affected by this incident. In an interesting move, VCU is also making attempts to remove this e-mail message from the student e-mail accounts.

---

### Links:

[1] <http://www.vcu.edu>

[2] <http://www.adamdodge.com/esi>

[3]

[http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD\\_BasicArticle&%09s=1045855935258&c=MGArticle&cid=1149192095252&path=!news!education](http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&%09s=1045855935258&c=MGArticle&cid=1149192095252&path=!news!education)

## Audit Finds Statewide System Exposes Private Information

### Quick Facts

- Date: 12/11/2006
- Institution: [North Dakota University System](#) [1], [North Dakota State University](#) [2], [University of North Dakota](#) [3]
- Type of Incident: Unauthorized Disclosure
- Number Affected: Unknown
- Source: [ESI](#) [4]
- Abstract Source: [In-Forum News](#) [5] (Free registration required)

### Abstract

A recent audit of the North Dakota State University System's ConnectND software revealed that personal student information is available to many individuals that should not have access to such information. ConnectND is the statewide system that North Dakota State Universities use to maintain information about state university students. The audit found that diverse individuals, including some student workers, have access to student information, including Social Security numbers. In addition, the audit raised serious questions about how credit card and other student financial information is stored within the system. University System officials say that the storage of credit cards was an oversight that is being fixed right away. As for access to Social Security numbers, officials are currently review university policies to see where changes can be made.

---

### Links:

[1] <http://www.ndus.nodak.edu/>

[2] <http://www.ndsu.nodak.edu/>

[3] <http://www.und.nodak.edu/>

[4] <http://www.adamdodge.com/esi>

[5] <http://www.in->

[forum.com/articles/index.cfm?id=149049&section=News&forumcomm\\_check\\_return&reebie\\_check&CFID=9988045&CFTOKEN=68458803&jsessionid=88308d4be3cf124644c5](http://forum.com/articles/index.cfm?id=149049&section=News&forumcomm_check_return&freebie_check&CFID=9988045&CFTOKEN=68458803&jsessionid=88308d4be3cf124644c5)

# UCLA Breach Exposes Almost One Million Identities

## Quick Facts

- Date: 12/12/2006
- Institution: University of California, Los Angeles [1]
- Type of Incident: Penetration
- Number Affected: 800,000
- Source: ESI [2]
- Abstract Source: Washington Post [3]

## Abstract

UCLA began notifying 800,000 current and former students, faculty and staff that their personal information, including Social Security numbers, names and addresses, might have been exposed in a recently discovered security breach. Computer security technicians recently uncovered a number of suspicious queries in a databases containing this personal information. It appears the intruder was able to exploit an unknown flaw in the database software to bypass security restrictions and gain access. Even though investigations so far show only a small number of Social Security numbers were accessed, UCLA is urging all 800,000 individuals to contact the three major credit bureaus and monitor their credit reports closely.

---

## Links:

[1] <http://www.ucla.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://www.washingtonpost.com/wp-dyn/content/article/2006/12/12/AR2006121200173.html>

# University of Texas Breach Exposes Student and Staff Information

## Quick Facts

- Date: 12/12/2006
- Institution: University of Texas, Dallas [1]
- Type of Incident: Penetration
- Number Affected: 5,000
- Source: ESI [2]
- Abstract: Dallas Business Journal [3]

## Abstract

The University of Texas, Dallas discovered that an unknown individual had gained unauthorized access to at least one UT Dallas computer. This intruder had access to a system(s) containing personal student and staff information including names, phone numbers, addresses and Social Security numbers. UT Dallas staff believe that the attack originated from the Internet, but declined to comment further because of the ongoing investigation. UT Dallas has put up a web site at [www.utdallas.edu/datacompromise/form.html](http://www.utdallas.edu/datacompromise/form.html) [4] for any student or staff member worried about their personal information.

---

## Links:

[1] <http://www.utdallas.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://charlotte.bizjournals.com/dallas/stories/2006/12/11/daily16.html>

[4] <http://www.utdallas.edu/datacompromise/form.html>

## UT Dallas Announces Breach Is Wider Than Initially Thought

### Quick Facts

- Date: 12/13/2006
- Institution: University of Texas, Dallas [1]
- Type of Incident: Penetration
- Number Affected: 1,000 additional (6,000 total)
- Source: ESI [2]
- Abstract Source: Dallas Business Journal [3]

### Abstract

University of Texas, Dallas officials announced that the recent breach suffered by the institution affected more individuals than was originally reported. After further investigation, it was uncovered that all individuals employed by the university between 1999 and 2005 had their personal information potentially exposed to an unknown attacker. This announcement raises the total number of individuals affected from 5,000 to 6,000.

---

### Links:

[1] <http://www.utdallas.edu>

[2] <http://www.adamdodge.com/esi>

[3] <http://dallas.bizjournals.com/dallas/stories/2006/12/11/daily31.html>

# UVa Faculty Urged To Destroy All Computer Data After Recent Incident

## Quick Facts

- Date: 12/14/2006
- Institution: [University of Virginia](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 62
- Source: [ESI](#) [2]
- Abstract Source: [Daily Progress](#) [3]

## Abstract

University of Virginia officials are asking all faculty to destroy any computer files or media that contain student's Social Security numbers. This move comes after the university suffers its second accidental disclosure of student SSNs. In this most recent incident, a teaching assistant accidentally e-mailed a spreadsheet containing names, grades and Social Security numbers to all 61 students in their class. While the university is in the process of phasing out the use of Social Security numbers as student identifiers, this will not happen until a new database system is installed. Currently, the university does not expect to have this new system installed and ready to use for another three years.

---

## Links:

[1] <http://www.virginia.edu>

[2] <http://www.adamdodge.com/esi>

[3]

[http://www.dailyprogress.com/servlet/Satellite?pagename=CDP%2FMGArticle%2FCDP\\_BasicArticle&c=MGArticle&cid=1149192173518&path=!news](http://www.dailyprogress.com/servlet/Satellite?pagename=CDP%2FMGArticle%2FCDP_BasicArticle&c=MGArticle&cid=1149192173518&path=!news)

## UC-Boulder Web Site Exploit Exposes 17,500 Student Records

### Quick Facts

- Date: 12/15/2006
- Institution: University of Colorado, Boulder [1]
- Type of Incident: Penetration
- Number Affected: 17,500
- Source: Attrition.org [2]
- Abstract: University of Colorado [3]

### Abstract

The University of Colorado at Boulder has begun to notify 17,500 students that an attacker was able to gain unauthorized access to a computer in the UC Boulder College of Arts and Sciences. This computer was used for advisement purposes and contained personal student information including names and Social Security numbers. According to the university officials, the attacker was able to gain access through a web site hosted on the computer. UC Boulder is still investigating this incident and is not aware of exactly what information was exposed during this attack at this point. UC Boulder stopped using SSNs for student identification back in 2005 and is currently deploying a complex program to search for any electronic records that still contain these numbers. The university has created a web page (<http://www.colorado.edu/its/security/awareness/privacy/identitytheft.pdf> [4]) to help answer any questions students might have about the incident or how to protect themselves from Identity Theft.

---

### Links:

[1] <http://www.colorado.edu>

[2] <http://www.attrition.org/dataloss>

[3] <http://www.colorado.edu/news/releases/2006/437.html>

[4] <http://www.colorado.edu/its/security/awareness/privacy/identitytheft.pdf>

## Student Information "Inadvertently" Left Exposed On Public Website

### Quick Facts

- Date: 12/19/2006
- Institution: [Mississippi State University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 2,400
- Source: [ESI](#) [2]
- Abstract Source: [The Clarion Ledger](#) [3]

### Abstract

Mississippi State University officials announced today that the personal information of 2,400 student workers was inadvertently posted to a public university web site. Included among this information were student names and Social Security numbers. The university has already contacted the affected students and has offered them one year of free credit monitoring. According to officials, the university is investigating the incident and removed the information immediately, but declined to name the department responsible for the exposure.

---

### Links:

[1] <http://www.msstate.edu>

[2] <http://www.adamdodge.com/esi>

[3]

<http://www.clarionledger.com/apps/pbcs.dll/article?AID=/20061219/NEWS/61219032>

## University Transmits 15,000 Tax Forms Over Non-Secured Connection

### Quick Facts

- Date: 12/22/2006
- Institution: [Texas Woman's University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 15,000
- Source: [ESI](#) [2]
- Abstract Source: [The Dallas Morning News](#) [3]

### Abstract

Texas Woman's University alerted all 15,000 students that were enrolled during the 2005 calendar year at the university's Denton, Dallas and Houston campuses to the possibility that their personal information was exposed this week. It seems the university transmitted all of these students' IRS 1098-T Tuition Statement information to an authorized vendor over an unsecured connection. While the university does not have any evidence that this information was exposed to an unauthorized party, officials point out that the university is aware of the potential for such and is taking the matter quite seriously. TWU has setup a both a "Data Exposure Response Hotline", 940-898-3840, and a "Data Exposure Response" web site, <http://www.twu.edu/response/index.asp> [4].

---

### Links:

[1] <http://www.twu.edu>

[2] <http://www.adamdodge.com/esi>

[3]

<http://www.dallasnews.com/sharedcontent/dws/dn/education/stories/122306dnmettwuidt.heft.3626d6f5.html>

[4] <http://www.twu.edu/response/index.asp>

# Yahoo Search Returns Faculty, Student Social Security Numbers

## Quick Facts

- Date: 12/22/2006
- Institution: [Utah Valley State College](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 15,000
- Source: [Attrition.org](#) [2]
- Abstract Source: [UVSC News Release](#) [3]

## Abstract

Utah Valley State College is working to notify 15,000 Distance Education faculty members and students about a recent security incident that exposed the names, Social Security numbers and other personal information of these individuals. Earlier this month, UVSC became aware that the personal information of individuals involved in the college's Distance Education program was starting to show up on the Yahoo search engine. UVSC immediately removed the information from its web servers and worked with Yahoo officials to remove the information from Yahoo as well. UVSC officials are confident the information is no longer publicly available. UVSC has setup both a hotline, 801-863-8200, and a web site, [www.uvsc.edu/it/idalert.htm](http://www.uvsc.edu/it/idalert.htm) [4], for anyone that has questions about this incident.

---

## Links:

[1] <http://www.uvsc.edu/>

[2] <http://www.attrition.org/dataloss>

[3] <http://resource.uvsc.edu/pressreleases/2006/22dec06.html>

[4] <http://www.uvsc.edu/it/idalert.html>