

EDUCATIONAL SECURITY INCIDENTS (ESI) YEAR IN REVIEW - 2009

RELEASED: JUNE 1, 2010

AUTHOR: ADAM DODGE

Copyright (c) Adam Dodge (unless otherwise noted), all rights reserved

Permission is granted for this material to be shared for noncommercial, educational purposes, provided that the material appears unaltered and credit is given to the author. To disseminate otherwise or to republish requires written permission from the author.

CONTENTS

Part 1: Introduction	1
Background.....	2
Definitions.....	3
Sources	5
Part 2: Overview.....	6
A Review of 2009	6
A Comparison to 2008, 2007 and 2006	8
Part 3: 2009 Facts and Figures.....	12
Incidents by Type of Incident	13
Incidents by Type – Employee Fraud.....	14
Incidents by Type – Impersonation	15
Incidents by Type – Penetration	16
Incidents by Type – Theft	18
Incidents by Type – Unauthorized Disclosure.....	19
Incidents by Type – Unknown	20
Incidents by Type of Information Exposed	21
Type of Information – Educational	22
Type of Information – Financial.....	23
Type of Information – Medical	24
Type of Information – Personally Identifiable.....	25
Type of Information – Social Security Number.....	28
Type of Information – Usernames and Passwords	31
Institutions Affected	32
Part 4: Educational Security Incidents.....	35
Former Clemson Official Alleges University Sold Computers Containing Private Data	36
Over 400 Social Security Numbers Stolen From University of Rochester Database	37
University of Oregon Laptop Containing Personal Information Stolen	38
Hundreds At Risk After Southwestern Oregon Community College Laptop Theft	39
LDAP Configuration Error Puts Social Security Numbers At Risk.....	40
Email Attachment Exposes Missouri State University Foreign Student Information.....	41
K-State Finds Student Information Online Since 2001.....	42
Email Leaks Ball State Employee Social Security Numbers	43
Drake University Academic Records Inadvertently Released.....	44
Breached Trent University Server Contained Personal Information.....	45
Mistake Sends Purdue 1099 Forms To Wrong Individuals.....	46
Seventeen Servers Breached at University of Alabama	47
BCC Alumni Magazine Covers Contain Social Security Numbers	48
University of Florida Breach Potentially Exposes Information Of 97,000 Individuals.....	49
Del Mar Class Roster With Social Security Numbers Stolen From Car	50
Software Error Exposes Ryerson Student Information.....	51
Police Allege Former IT Admin Stole Nude Facebook Pictures	52

Library Patron Data At Risk After Sever Breach	53
Stolen University of Toledo Computer Contains Student and Faculty Information	54
Virus Prompts Penn State Breach Notification	55
University Notifies Students, Faculty Over Summer Laptop Theft	56
Huron Staff Working To Notify Current, Former Students After Server Breach	57
Security Incident Prompts Shredding Change at SCC.....	58
Abilene Christian University Server Breached	59
Pacific University Laptop Containing Sensitive Information Missing	60
Owensboro Community and Technical College Missing Hard Drive Contains Student Information.....	61
Massey University Error Allows Students To Access Personal Information Of Others	62
University of Washington Breaches Exposes Worker Information	63
Brigham Young University Email Error Sends Student IDs and GPAs To All Students	64
Potential Breach At Penn State Behrend	65
National University of Singapore Email Leaks Alumni Data.....	66
TWU Degree Auditing System Error Exposes Student Course, Grades.....	67
Malware Infects Kapiolani Community College Compute With Access To Sensitive Information.....	68
Hackers Breach UC Berkeley Database, Steal Social Security Numbers	69
User Web Site Security Failure Leads To Ball State Breach.....	70
Stolen UAMS Computer Contained Current, Former Employee Information	71
UNLV Notifies Students Over Potential Data Leak	72
Virginia Commonwealth University Notifies Students About Possible Breach	73
Email Attachment Contains the Social Security Numbers of 350 OSU Student Workers	74
Oregon Health & Science University Notifies Patients After Laptop Theft	75
Kirkwood Community College Warns of Potential Data Breach.....	76
Laptop Containing University of North Dakota Donor Information Stolen From Contractor	77
Johns Hopkins University's Applied Physics Laboratory's Web Site Breached	78
Stolen Cornell Laptop Contains Sensitive Information on Students, Faculty and Staff	79
Oregon University System's Web Site Replaced With Angry Message About Iran	80
Stolen UCM Reports Contain Information on 7,000 Students	81
UCSD Flooded With Phone Calls Following Computer	82
Former Professor Suspected in KU Laptop Theft.....	83
Stolen UCCS Laptop Contained Student Information	84
UTB Staff Abuse Access To Blackboard To Cheat.....	85
Degree Auditing System Security Lapse Makes University of Oregon GPAs Visible Online.....	86
Berkeley School of Journalism Web Site Breach Exposes Student Information	87
LSU Web Site Exposes Student Information.....	88
Stolen NKU Laptop Contains Current, Former Student Information.....	89
Massive Computer Theft Raises Identity Theft Concerns at CSULA	90
File Sharing Program on BU ROTC Computer Exposes Personal Information	91
UMass Computer Breach Exposes 20 Years Of Personal Data.....	92
UMass Computer Breach Exposes 20 Years Of Personal Data	93
University of Vermont Announces Credit Card Breach	94
Security Breach at University of Florida	95
EKU Social Security Numbers Online For A Year	96
[Update1]Server Containing UNC-Chapel Hill Study Breached	97

Stolen Williams College Laptop Contained Personal Information	98
Email Attachment Contains Suffolk Student Social Security Number	99
Breach Causes Shutdown of Tufts WebCenter	100
Email Hoax Traced to University of Colorado Denver	101
Student and Staff Information Stolen From Roane State Employee's Car	102
Multi-Computer University of Wisconsin-Madison Breach Exposes Personal Information	103
CSULA Faculty Member Mistakenly Posts Files With Student Data Online	104
Student and Alumni Data On Stolen Bloomsburg University	105
Mistake Exposes Personal Information of Chaminade University Students	106
Cal Poly Pomona Applicant Information Online For Five Years	107
University of East Anglia Climate Research Center Servers Hacked	108
[Update1] Employee Information Available on Notre Dame Web Site	109
University College Dublin Hands Media Confidential Student Information	110
Nebraska Lincoln Computer Breach Affects High School graduates	111
Eastern Illinois University Admissions Server Compromised By Virus	112
Valdosta Investigates Server Breach	113
Daytona State College Email System Hacked, Used to Send Bomb Threats	114
UCSF Doctor Falls Victim to Phishing Scam	115
North Carolina Colleges Library System Breached	116
[UPDATE1] Malware Potentially Exposes Penn State Student Information	118
Western Michigan University Web Site Accidentally Exposes Student Information	119
Eastern Washington University Breach Affects 130,000	120

TABLE OF FIGURES

Figure 1: 2009 Incident Breakdown by Type	6
Figure 2: Number of Incidents by Information Exposed	7
Figure 3: Number of Incidents Reported	8
Figure 4: Number of Institutions Affected by Incidents.....	9
Figure 5: Number of Incidents by Type of Incident 2006-2009.....	10
Figure 6: Number of Incidents by Information Exposed 2006-2009.....	11

TABLE OF TABLES

Table 1: Changes in Incidents Reported 2006-2009.....	10
Table 2: Change in Type of Incident by Information Exposed 2006-2009.....	11
Table 3: Breakdown of Incidents by Type.....	13
Table 4: Average Number of Records per Incident.....	13
Table 5: Chronological List of Employee Fraud Incidents	14
Table 6: Chronological List of Impersonation Incidents	15
Table 7: Chronological List of Penetration Incidents	16
Table 8: Chronological List of Theft Incidents.....	18
Table 9: Chronological List of Unauthorized Disclosure Incidents	19
Table 10: Chronological List of Unknown Incidents.....	20
Table 11: Breakdown of the Number of Incidents and Records Affected by Type of Information Exposed.....	21
Table 12: Chronological List of Incidents Exposing Educational Information	22
Table 13: Chronological List of Incidents Exposing Financial Records.....	23
Table 14: Chronological List of Incidents Exposing Medical Records	24
Table 15: Chronological List of Incidents Exposing Personally Identifiable Records	25
Table 16: Chronological List of Incidents Exposing Social Security Number Records	28
Table 17: Alphabetical List of Institutions	32

PART 1: INTRODUCTION

The Educational Security Incidents (ESI) Year in Review – 2009 is a look at the information security breaches that occurred during 2009 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 – 2009 is broken into four main parts: The Introduction, Overview, Facts and Figures, and the Educational Security Incidents.

The Introduction explains the reasoning and purpose behind ESI and the ESI Year in Review – 2009 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 – 2009, Overview, examines the changes in the reported breaches of 2009. The Overview also contains a comparison of breaches between 2009, 2008, 2007 and 2006. This comparison includes a look at the changes in the total number of breaches reported and total number of institutions reporting breaches. This section closes with a look at the changes in the number of incidents by type of information exposed.

The third part of the ESI Year in Review – 2009, 2009 Facts and Figures, looks at educational security incidents in aggregate. From this total collection, 2009 Facts and Figures examines the impact different types of incidents had during 2009. The 2009 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 rundown of all institutions that reported an information security breach during 2009.

The final part of the ESI Year in Review – 2009, the Educational Security Incidents, is a collection of all information security write-ups from 2009 as collected by ESI. The write-ups are included as an easy-to-browse collection of all reported educational security incidents that occurred in 2009. In addition, the write-ups serve as evidence for the information contained in the Overview and 2009 Facts and Figures sections 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 that exist to educational information and information systems.

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 occur with higher education 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 of incidents, 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. ESI 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(s) 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 2009 educational security incidents are broken down between seven different incident types adopted from the Classification Codes Dr. M. E. Kabay developed for the INFOSEC Year in Review¹. These seven types are:

- Employee Fraud – Incidents involving fraudulent activity by employees
- 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
- Penetration – Incidents involving the breach of computer software, a computer system or a computer network
- Theft – Incidents involving the theft of physical mediums such as drives, equipment or printouts
- Unauthorized Disclosure – Incidents involving the release of information to unknown and/or unauthorized individuals
- Unknown – Incidents involving an unknown cause

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 six different types. These six types of information are:

- Educational – Contains the educational information of an individual including class schedule and grade information
- Financial – Contains the financial information of an individual including bank accounts, checking information and credit card numbers
- Medical – Contains the medical information of an individual
- Personally Identifiable – Contains information that belongs to an individual, but not necessarily private such as name, address, birth date, e-mail address, etc.

¹ A current list of Dr. Kabay's Classification Codes can be found at <http://www.mekabay.com/iyir/index.htm>

- Social Security Numbers – The Social Security number of an individual (or the equivalent if the incident occurred outside of the United States)
- Usernames and Passwords – Contains the access credentials of an individual to an information resource

SOURCES

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

- A Chronology of Data Breaches (www.privacyrights.org/ar/ChronDataBreaches.htm), Privacy Rights Clearinghouse
- DataBreach.net, "Dissent", owner
- Data Loss Archive and Database (attrition.org/dataloss), Attrition.org Staff
- Identity Theft Resource Center (www.idtheftcenter.org), Linda Foley, et al.
- InfoSec News (www.infosecnews.org), William Knowles, moderator
- INFOSEC Year in Review (www2.norwich.edu/mkabay/iyr), Dr. M.E. Kabay, et al.
- OSF Data Loss Database (www.datalosssdb.org), Open Security Foundation
- PHIPrivacy.net, "Dissent", owner
- The RISKS Forum (catless.ncl.ac.uk/risks), Dr. Peter G. Neumann, moderator
- Security News Portal (www.securitynewsportal.com)
- SSNBreach.org (www.ssnbreach.org), Aaron Titus
- Student, Local and National News Outlets

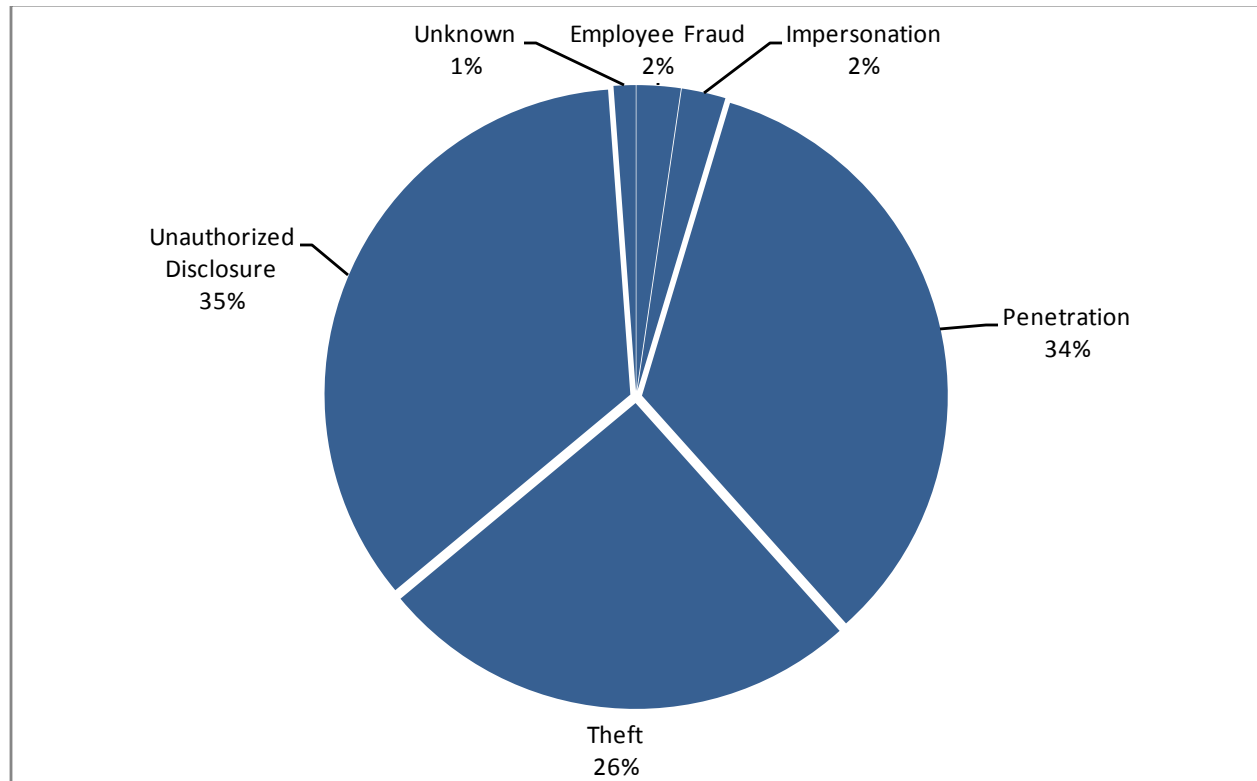
PART 2: OVERVIEW

The information security incidents reported by institutions of higher education throughout 2009 were down significantly in both the number of incidents and the amount of information exposed. This downward trend in higher education incidents follows a broader downward trend in breaches across all industry sectors in 2009². As such, 2009 saw fewer institutions reporting a smaller number of breaches. During 2009, institutions of higher education showed no Loss-type incidents, a significant change over the past three years. In addition, only one incident reported in the news affected multiple institutions, a substantially smaller number than 2008. However, the large number of institutions involved in this one multi-institution incident once again caused the number of institutions suffering from a breach to be greater than the number of breaches reported.

A REVIEW OF 2009

As shown in Figure 1 below, the Unauthorized Disclosure of information to individuals not authorized to view such data continues to be the leading type of information security incident that colleges and universities suffer. This is a trend that started in 2007 and continues through 2009, if only by the smallest of margins. Penetration moved from the third to the second most common type of security incident in 2009 while Theft of information and/or information resources dropped from second to third. All told, the top three most common types of incidents within higher education accounted for 95% of all of the incidents in 2009.

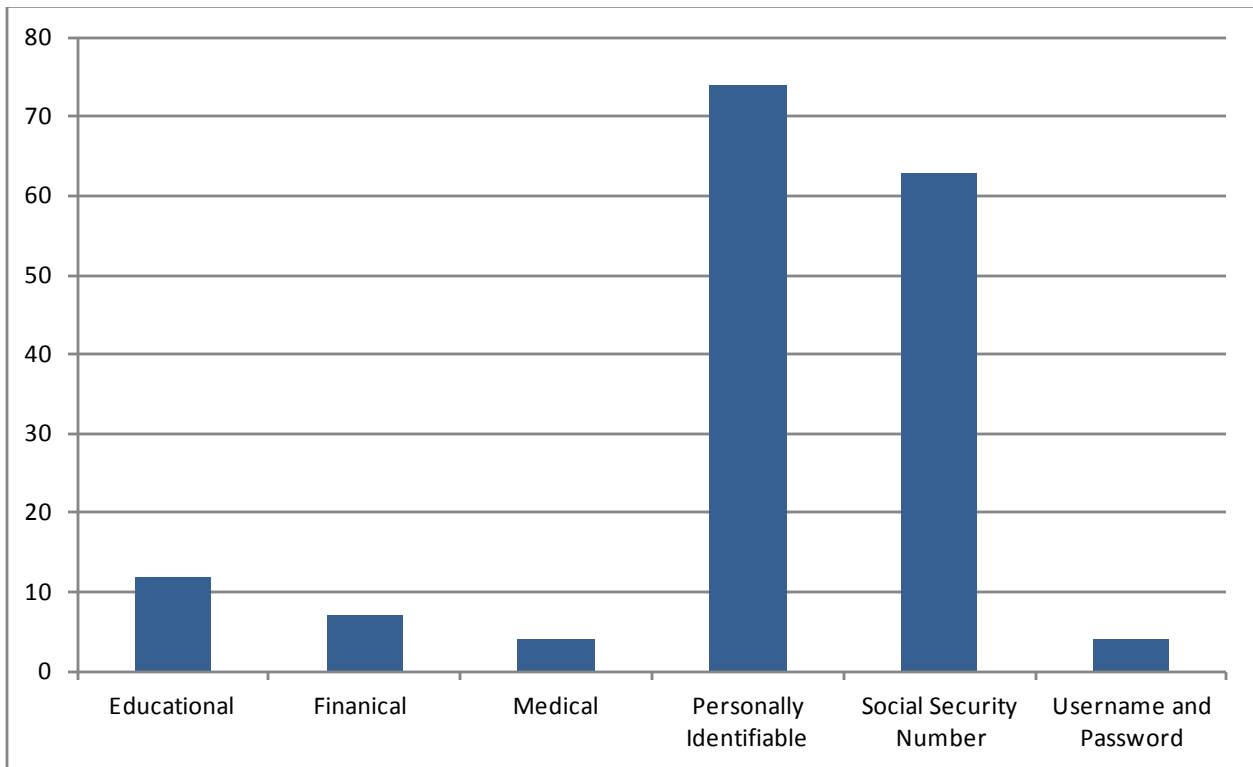
Figure 1: 2009 Incident Breakdown by Type



² Open Security Foundation's Data Loss DB's Data Loss Statistics: <http://datalossdb.org/statistics>

While employee mistakes continue to be the leading cause of security incidents at colleges and universities (as reported in the news), these mistakes no longer out number traditional “hacker” attacks (Penetration-type incidents) by as large of a margin. In fact, employee mistakes (i.e. Unauthorized Disclosure plus Loss) only lead to one more incident in 2009 than did Penetration of computer and network systems by an outside individual. Looking at the numbers, this change is due to a significant decrease in the number of Unauthorized Disclosure and Loss-type incidents then any real reduction on Penetration-types incidents as will be shown later.

Figure 2: Number of Incidents by Information Exposed

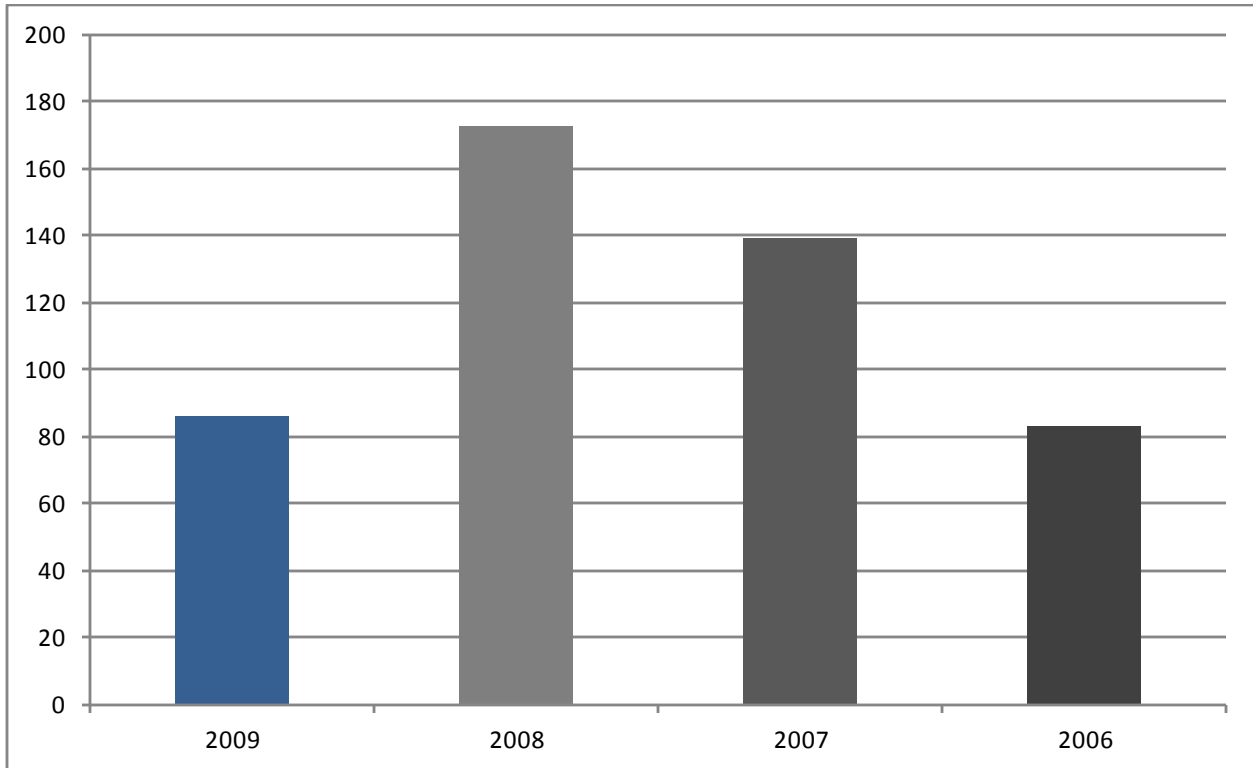


As has been the case since first ESI Year in Review, Personally Identifiable Information continues to be the most common information exposed during security incidents occurring within higher education. Following along on this same trend, Social Security Numbers continue to hold the number two spot in terms of information exposed during incidents at colleges and universities reported in the news. Given that most mandatory reporting laws involve these two information types, it is not surprising to find both at the top of the list of information exposure during higher education security incidents. As with 2008, there is a shocking difference in the number of incidents exposing Personally Identifiable information and/or Social Security Numbers and those exposing the other information types listed above. As stated last year, this could be caused by breach notification laws or it could be that colleges and universities continue to improve on the way they protect Educational, Financial and Medical information.

A COMPARISON TO 2008, 2007 AND 2006

As mentioned above, the number of information security incidents in 2009 decreased significantly over 2008. In fact, the number of security incidents reported in 2009 dropped to levels last seen in 2006, reversing the growth shown over 2007 and 2008.

Figure 3: Number of Incidents Reported



In addition to the decrease in the number of incidents reported in 2009, there was also a decrease in the number of institutions affected by incidents, as would be expected. While the number of institutions affected in 2009 is close to the number in 2007 as shown in Figure 4 below, this is caused by a single incident affecting a large number of institutions (25) simultaneously. If this single occurrence is removed, the number of institutions affected drops closer to 2006 levels.

Figure 4: Number of Institutions Affected by Incidents

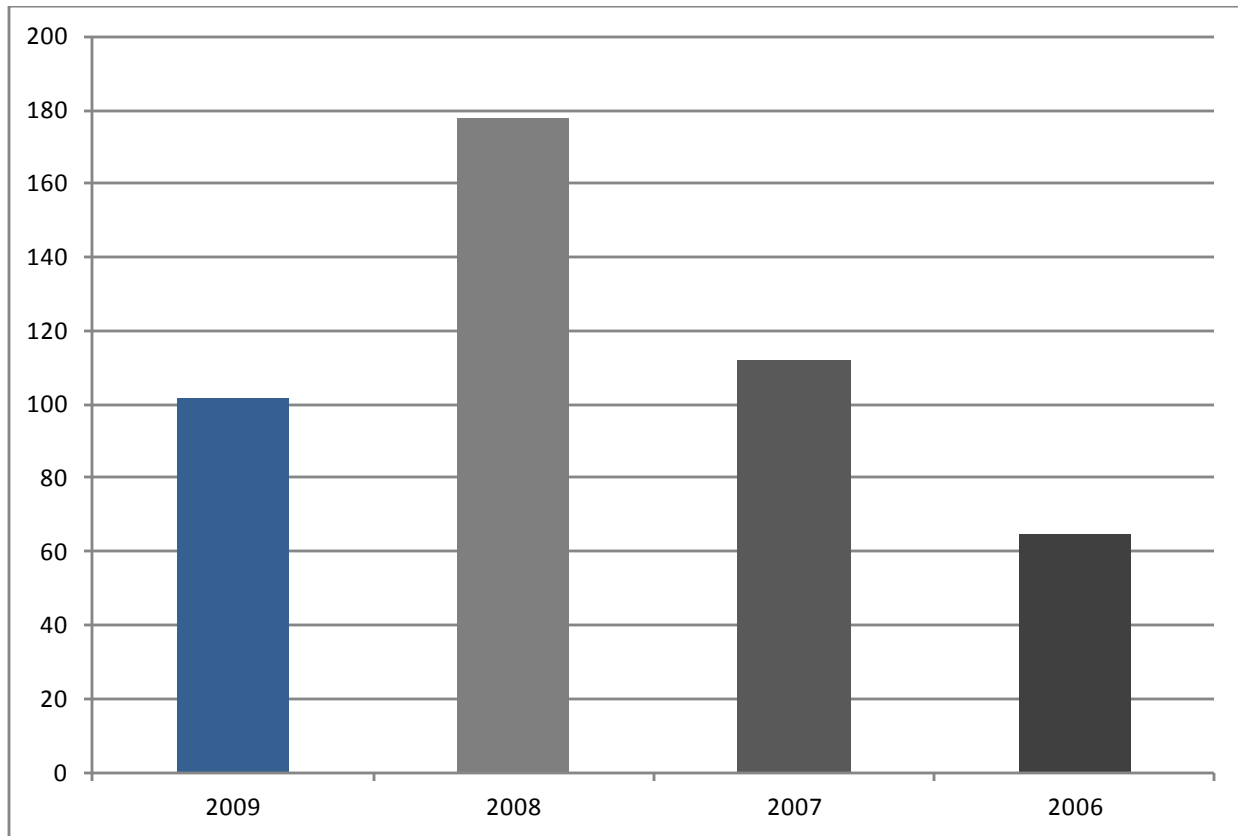
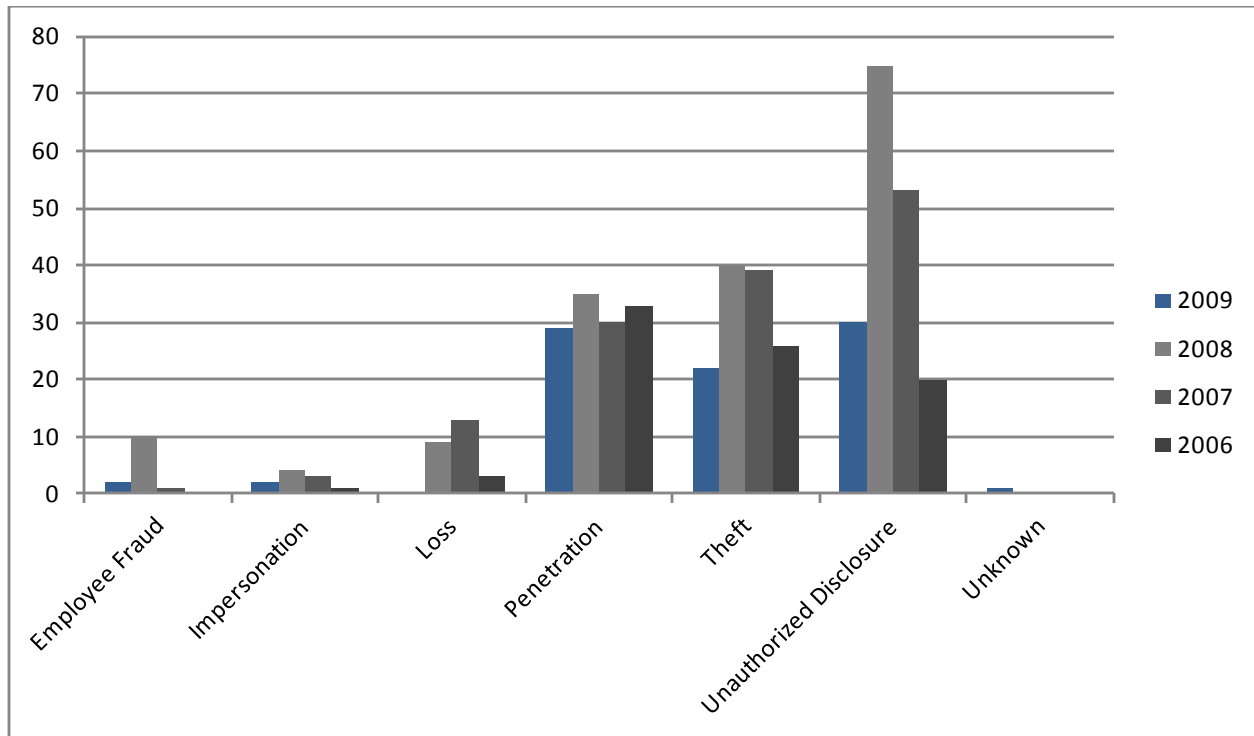


Figure 5: Number of Incidents by Type of Incident 2006-2009

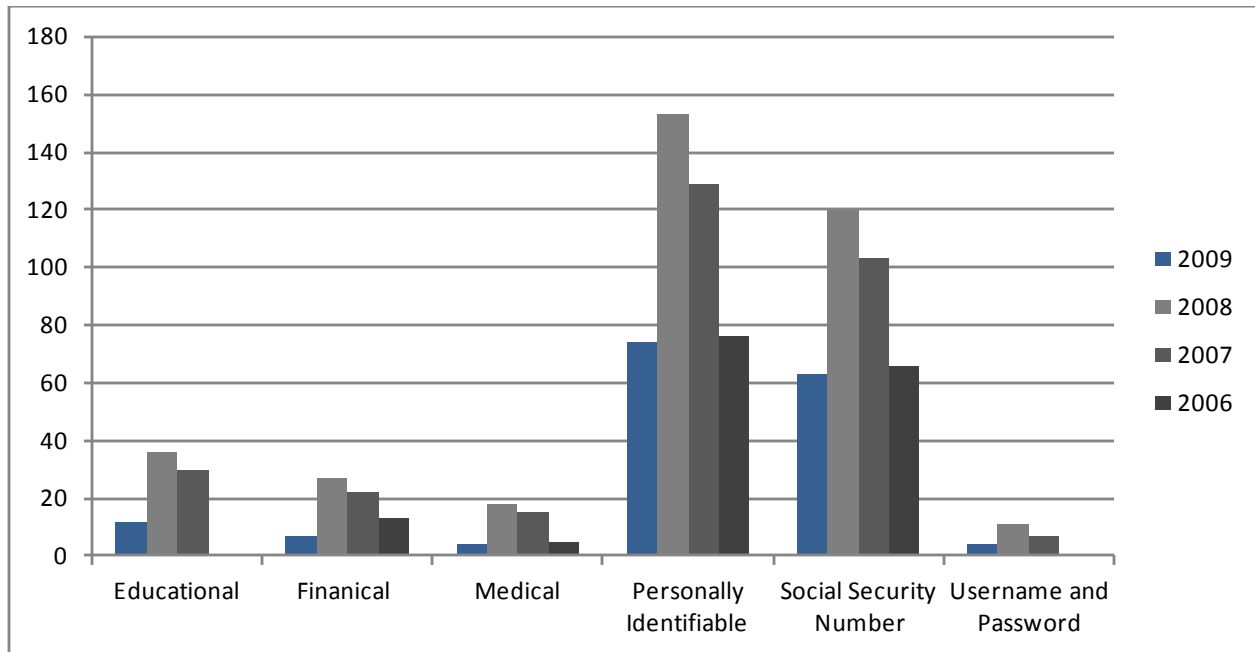


Looking at the number of incidents by type of incident (Figure 5), the same general decrease can be seen across all incident types. As mentioned earlier, some of the most significant drops are found in the Loss-type, which dropped to zero, and the Unauthorized Disclosure-type, which dropped by over 50% from 2008. The only incident type to increase is the Unknown-type, which is new to the Year in Review – 2009. The Unknown-type incident involves a university that was warned by its bank that a number of university credit cards had been compromised, but it was not reported as to how this happened. Interestingly, the number of Penetration-type incidents has remained relatively the same between 2006 and 2009. In fact the number of Penetration-type incidents varies by only six (6) incidents between the lowest year (2009) and the highest (2008) as shown below.

Table 1: Changes in Incidents Reported 2006-2009

Type of Incident	Reported In 2009	Reported In 2008	Reported In 2007	Reported In 2006
Employee Fraud	2	10	1	-
Impersonation	2	4	3	1
Loss	-	9	13	3
Penetration	29	35	30	33
Theft	22	40	39	26
Unauthorized Disclosure	30	75	53	20
Unknown	1	-	-	-
	86	173	139	83

Figure 6: Number of Incidents by Information Exposed 2006-2009



Looking at the number of incidents by the information-type exposed shows no surprise given the downward trend in 2009. Again there is a significant decrease across all information-types exposed during a security incidents reported in higher education in 2009. Looking at the data below, the numbers in 2009 are close to those reported in 2006.

Table 2: Change in Type of Incident by Information Exposed 2006-2009

Type of Information	Reported in 2009	Reported in 2008	Reported in 2007	Reported in 2006
<i>Educational</i>	12	36	30	1
<i>Financial</i>	7	27	22	13
<i>Medical</i>	4	18	15	5
<i>Personally Identifiable</i>	74	153	129	76
<i>Social Security Number</i>	63	120	103	66
<i>Username and Password</i>	4	11	7	0

PART 3: 2009 FACTS AND FIGURES

The following part of the ESI Year in Review – 2009 breaks down the information on reported security incidents to help better examine the incidents and the effects of these incidents. Part 3 of the Year in Review – 2009 is comprised of three sections relating to different aspects of each incident: Type of Incident, Type of Information Exposed, and Institutions Affected.

Type of Incident breaks down the reported security incidents by the type of event that occurred. This section places each incident into one of six incident types: Employee Fraud, Impersonation, Loss, Penetration, Theft, 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 six information types: Educational Information, Financial Information, Medical Information, Personally Identifiable Information, Social Security Numbers (or the foreign equivalent) and Username and Passwords. 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 – 2009 is simply an alphabetical list of the 102 colleges and universities that reported suffering one or more information security breach.

INCIDENTS BY TYPE OF INCIDENT

In 2009, 102 different educational institutions reported 86 different educational security incidents. These 86 incidents lead to the exposure of 1,043,532 records containing at least one type of sensitive and/or personal information. This total number of records includes 14 distinct incidents where there was no reporting on the number of records exposed. Below is a breakdown of the 2009 educational security incidents by the type of incident.

Table 3: Breakdown of Incidents by Type

Type of Incident	Number of Incidents	Number of Institutions Affected	Number of Records Exposed
Employee Fraud	2	2	16
Impersonation	2	2	1
Penetration	29	51 ³	773,722 ⁴
Theft	22	22	182,333 ⁵
Unauthorized Disclosure	30	29 ⁶	87,460 ⁷
Unknown	1	1	242
Grand Totals	86	102⁸	1,043,774⁹

Table 4: Average Number of Records per Incident

Type of Incident	Number of Incidents	Number of Records Exposed	Average Number of Records Per Incident ^{10 11}
Employee Fraud	2	16	8
Impersonation	2	1	1
Penetration	29	773,722	26,680
Theft	22	182,333	8,288
Unauthorized Disclosure	30	87,460	2,915
Unknown	1	242	242
Overall Average			12,137

³ One Penetration-type incidents affected multiple institutions

⁴ Penetration total includes four (4) incidents where the total number affected was not reported

⁵ Theft total includes four (4) incidents where the total number affected was not reported

⁶ At least one (1) institution reported multiple Unauthorized Disclosure-type incidents

⁷ Unauthorized Disclosure includes six (6) incidents where the total number affected was not reported

⁸ Several institutions suffered more than one incident causing the Grand Total to be lower than the sum by affected by incident type

⁹ Grand Total includes 14 incidents where the total number affected was not reported

¹⁰ Averages rounded to the nearest full number

¹¹ Average calculations might contain extraordinarily large incidents which may skew overall averages

INCIDENTS BY TYPE – EMPLOYEE FRAUD

Employee Fraud tied as the second to least common information security incident at colleges and universities as reported in the news. Overall, two institutions reported two cases of information exposure and/or loss related to fraudulent employee conduct. These two incidents accounted for the exposure of 16 records. Below is a chronological list of the Employee Fraud-type incidents that occurred during 2009.

Table 5: Chronological List of Employee Fraud Incidents

Date	Institution	Number Affected
3/2/2009	University of Massachusetts	16
8/1/2009	University of Texas, Brownsville	-
	Total	16

INCIDENTS BY TYPE – IMPERSONATION

Impersonation tied as the second to least common information security incident at colleges and universities as reported in the news. Overall, two institutions reported two cases of information exposure and/or loss related to impersonation. These two incidents accounted for the exposure of one records. Below is a chronological list of the Impersonation-type incidents that occurred during 2009.

Table 6: Chronological List of Impersonation Incidents

Date	Institution	Number Affected
10/9/2009	University of Colorado, Denver	-
12/11/2009	Daytona State College	1
	Total	1

INCIDENTS BY TYPE – PENETRATION

Penetration ranked as the second most common information security incident at colleges and universities as reported in the news. Overall, 51 institution reported 29 incidents involving exposure and/or loss related to the breaching of computer and network systems. These 29 incidents accounted for the exposure of 773,722 records including four incidents where the number of records exposed was not reported. Below is a chronological list of the Penetration-type incidents that occurred during 2009.

Table 7: Chronological List of Penetration Incidents

Date	Institution	Number Affected
1/11/2009	University of Rochester	450
2/9/2009	Trent University	21
2/14/2009	University of Alabama	37,000
2/19/2009	University of Florida	97,000
3/3/2009	Western Oklahoma State College	1,500
3/18/2009	Huron University College	25,000
3/26/2009	Abilene Christian University	<i>Unknown</i>
4/1/2009	University of Washington	6,000
4/9/2009	Pennsylvania State University, The Behrend College	10,868
5/4/2009	Kapiolani Community College	15,487
5/8/2009	University of California, Berkeley	160,000
5/22/2009	Ball State University	2,000
6/17/2009	Johns Hopkins University	-
6/24/2009	Oregon University System	-
7/17/2009	University of California, San Diego	30,000
8/11/2009	University of California, Berkeley	493
8/21/2009	University of Massachusetts, Amherst	<i>Unknown</i>
9/24/2009	University of North Carolina, Chapel Hill	160,000
10/6/2009	Tufts University	-
10/12/2009	University of Wisconsin, Madison	3,000
11/19/2009	University of East Anglia	<i>Unknown</i>
11/30/2009	Pennsylvania State University	303
12/4/2009	Eastern Illinois University	9,000
12/4/2009	University of Nebraska Lincoln	4,000
12/11/2009	Valdosta State University	<i>Unknown</i>
12/15/2009	University of California, San Francisco	600

12/17/2009	Alamance Community College, Beaufort County Community College, Bladen Community College, Blue Ridge Community College, Brunswick Community College, Central Carolina Community College, College of The Albemarle, Gaston College, Halifax Community College, Haywood Community College, Johnston Community College, Lenoir Community College, Martin Community College, Nash Community College, Pamlico Community College, Piedmont Community College, Richmond Community College, Roanoke-Chowan Community College, Rowan-Cabarrus Community College, Sandhills Community College, Southwestern Community College, Tri-County Community College, Vance-Granville Community College, Wake Tech Community College, Wilson Community College	51,000
12/18/2009	Pennsylvania State University	30,000
12/31/2009	Eastern Washington University	130,000
	Total	773,722¹²

¹² Total for Penetration-type incidents includes four incidents where the total number of records exposed was not reported

INCIDENTS BY TYPE – THEFT

Theft ranked as the third most common information security incident at colleges and universities as reported in the news. Overall, 22 institutions reported 22 incidents involving exposure and/or loss related to the theft of information and/or information resources. These 22 incidents accounted for the exposure of 182,333 records including four incidents where the number of records exposed was not reported. Below is a chronological list of the Theft-type incidents that occurred during 2009.

Table 8: Chronological List of Theft Incidents

Date	Institution	Number Affected
11/1/2009	Bloomsburg University of Pennsylvania	574
8/31/2009	Bluegrass Community and Technical College	100
8/18/2009	California State University, Los Angeles	600
6/23/2009	Cornell University	45,277
2/20/2009	Del Mar College	53
7/23/2009	Kansas University	<i>Unknown</i>
6/12/2009	Kirkwood Community College	1,600
8/15/2009	Northern Kentucky University	200
6/12/2009	Oregon Health & Science University	1,000
3/31/2009	Owensboro Community and Technical College	3,000
3/28/2009	Pacific University	<i>Unknown</i>
10/12/2009	Roane State Community College	10,941
1/16/2009	Southwestern Oregon Community College	200
5/30/2009	University of Arkansas for Medical Sciences	<i>Thousands</i>
6/26/2009	University of Central Missouri	7,000
7/28/2009	University of Colorado at Colorado Springs	766
6/17/2009	University of North Dakota	84,000
1/13/2009	University of Oregon	<i>Unknown</i>
3/16/2009	University of Toledo	24,450
3/18/2009	University of West Georgia	1,300
6/5/2009	Virginia Commonwealth University	22,500 (Test), 17,214 (SSN)
10/3/2009	Williams College	750
	Total	181,333¹³

¹³ Total for Theft-type incidents includes four incidents where the total number of records exposed was not reported

INCIDENTS BY TYPE – UNAUTHORIZED DISCLOSURE

Unauthorized Disclosure ranked as the most common information security incident at colleges and universities as reported in the news. Overall, 29 institutions reported 30 incidents involving information exposure and/or loss related to release of information to the public and/or individuals not authorized to view such information. These 30 incidents accounted for the exposure of 87,460 records including six incidents where the number of records exposed was not reported. Below is a chronological list of the Unauthorized Disclosure-type incidents that occurred during 2009.

Table 9: Chronological List of Unauthorized Disclosure Incidents

Date	Institution	Number Affected
2/4/2009	Ball State University	19
8/20/2009	Boston University	6,675
4/2/2009	Brigham Young University	<i>Unknown</i>
2/17/2009	Broome Community College	14,000
11/15/2009	California State Polytechnic University, Pomona	355
10/14/2009	California State University, Los Angeles	85
11/6/2009	Chaminade University	4,500
1/5/2009	Clemson University	<i>Unknown</i>
2/9/2009	Drake University	800
9/24/2009	Eastern Kentucky University	5,045
1/30/2009	Kansas State University	45
8/13/2009	Louisiana State University	<i>Unknown</i>
4/1/2009	Massey University	200
9/29/2009	Memorial University of Newfoundland	<i>Unknown</i>
1/21/2009	Missouri State University	565
4/20/2009	National University of Singapore	15,794
11/20/2009	Notre Dame	24,000
6/8/2009	Ohio State University	350
3/17/2009	Pennsylvania State University	1,000
2/9/2009	Purdue University	962
2/23/2009	Ryerson University	588
3/21/2009	Solano Community College	<i>Unknown</i>
10/4/2009	Suffolk Community College	300
4/25/2009	Texas Woman's University	12,000
11/24/2009	University College Dublin	2
1/20/2009	University of Florida	101
9/14/2009	University of Florida	34
6/1/2009	University of Nevada, Las Vegas	20
8/2/2009	University of Oregon	20
12/22/2009	Western Michigan University	<i>Unknown</i>
	Total	87,460¹⁴

¹⁴ Total for Unauthorized Disclosure-type incidents includes six incidents where the total number of records exposed was not reported

INCIDENTS BY TYPE – UNKNOWN

Unknown is new to the ESI Year in Review for 2009 and ranked as the least common information security incident at colleges and universities as reported in the news. Overall, one institution reported one incidents involving information exposure and/or loss related to unknown reasons. This one incident accounted for the exposure of 242 records. Below is a chronological list of the Unknown-type incidents that occurred during 2009.

Table 10: Chronological List of Unknown Incidents

Date	Institution	Number Affected
9/2/2009	University of Vermont	242
	Total	242

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. In this section, each “record” represents a specific piece of information about an individual. Therefore, each Type of Incident record could contain multiple Type of Information records leading to a higher Type of Information incident and record total.

Table 11: Breakdown of the Number of Incidents and Records Affected by Type of Information Exposed

Type of Information	Number of Incidents	Number of Records Affected
Educational	12	36,085 ¹⁵
Financial	7	100,470 ¹⁶
Medical	4	191,600
Personally Identifiable	74	1,063,493 ¹⁷
Social Security Number	63	1,028,350 ¹⁸
Username and Password	4	17 ¹⁹

¹⁵ Educational total includes two incidents where the total number of records affected was not reported

¹⁶ Financial total includes two incidents where the total number of records affected was not reported

¹⁷ Personally Identifiable total includes 11 incidents where the total number of records affected was not reported

¹⁸ Social Security Number total includes nine incidents where the total number of records affected was not reported

¹⁹ Username and Password total includes two incidents where the total number of records affected was not reported

TYPE OF INFORMATION – EDUCATIONAL

Educational information ranked as the third most common type of information exposed during information security incidents at colleges and universities as reported in the news. Overall, 12 information security incident exposed 36,085 records containing Educational information such student grades and class schedules including two incidents where the number affected was not reported. Below is a chronological list of all incidents exposing Educational Records information that occurred during 2009.

Table 12: Chronological List of Incidents Exposing Educational Information

Date	Institution	Number Affected
4/1/2009	Massey University	200
4/2/2009	Brigham Young University	<i>Unknown</i>
4/20/2009	National University of Singapore	15,794
4/25/2009	Texas Woman's University	12,000
7/28/2009	University of Colorado at Colorado Springs	766
8/1/2009	University of Texas, Brownsville	0
8/2/2009	University of Oregon	20
10/12/2009	University of Wisconsin, Madison	3,000
11/24/2009	University College Dublin	2
11/30/2009	Pennsylvania State University	303
12/4/2009	University of Nebraska Lincoln	4,000
12/11/2009	Valdosta State University	<i>Unknown</i>
	Total	36,085²⁰

²⁰ Total number of Educational records exposed includes two incidents where the total number of records exposed was not reported

TYPE OF INFORMATION – FINANCIAL

Financial information ranked as the third least common type of information exposed during information security incidents at colleges and universities as reported in the news. Overall, seven information security incidents exposed 100,470 records containing Financial information such as credit card and bank account numbers including two incidents where the number affected was not reported. Below is a chronological list of all incidents exposing Financial Records information that occurred during 2009.

Table 13: Chronological List of Incidents Exposing Financial Records

Date	Institution	Number Affected
2/9/2009	Trent University	21
2/9/2009	Purdue University	962
5/4/2009	Kapiolani Community College	15,487
6/17/2009	University of North Dakota	84,000
8/21/2009	University of Massachusetts, Amherst	<i>Unknown</i>
9/2/2009	University of Vermont	-
9/29/2009	Memorial University of Newfoundland	<i>Unknown</i>
	Total	100,470²¹

²¹ Total number of Financial records exposed includes two incidents where the total number of records exposed was not reported

TYPE OF INFORMATION – MEDICAL

Medical information tied as the least common type of information exposed during information security incidents at colleges and universities as reported in the news. Overall, 4 incidents exposed 191,600 records containing Medical information such as diagnosis and treatment information. Below is a chronological list of all incidents exposing Medical Records information that occurred during 2009.

Table 14: Chronological List of Incidents Exposing Medical Records

Date	Institution	Number Affected
5/8/2009	University of California, Berkeley	160,000
6/12/2009	Oregon Health & Science University	1,000
7/17/2009	University of California, San Diego	30,000
12/15/2009	University of California, San Francisco	600
	Total	191,600

TYPE OF INFORMATION – PERSONALLY IDENTIFIABLE

Personally Identifiable information ranked as the most common type of information exposed during information security incidents at colleges and universities as reported in the news. Overall, 74 incidents exposed 1,063,493 records containing Personally Identifiable information such as names, dates of birth, addresses, and e-mail addresses including 11 incidents where the number exposed was not reported. Below is a chronological list of all incidents exposing Personally Identifiable information that occurred during 2009.

Table 15: Chronological List of Incidents Exposing Personally Identifiable Records

Date	Institution	Number Affected
1/5/2009	Clemson University	<i>Unknown</i>
1/11/2009	University of Rochester	450
1/13/2009	University of Oregon	<i>Unknown</i>
1/16/2009	Southwestern Oregon Community College	200
1/20/2009	University of Florida	101
1/21/2009	Missouri State University	565
1/30/2009	Kansas State University	45
2/4/2009	Ball State University	19
2/9/2009	Drake University	800
2/9/2009	Trent University	21
2/9/2009	Purdue University	962
2/14/2009	University of Alabama	37,000
2/17/2009	Broome Community College	14,000
2/19/2009	University of Florida	97,000
2/20/2009	Del Mar College	53
2/23/2009	Ryerson University	588
3/3/2009	Western Oklahoma State College	1,500
3/16/2009	University of Toledo	24,450
3/17/2009	Pennsylvania State University	1,000
3/18/2009	University of West Georgia	1,300
3/18/2009	Huron University College	25,000
3/21/2009	Solano Community College	<i>Unknown</i>
3/28/2009	Pacific University	<i>Unknown</i>
3/31/2009	Owensboro Community and Technical College	3,000
4/1/2009	Massey University	200
4/1/2009	University of Washington	6,000
4/2/2009	Brigham Young University	<i>Unknown</i>
4/9/2009	Pennsylvania State University, The Behrend College	10,868
4/20/2009	National University of Singapore	15,794
4/25/2009	Texas Woman's University	12,000
5/4/2009	Kapiolani Community College	15,487
5/8/2009	University of California, Berkeley	160,000
5/30/2009	University of Arkansas for Medical Sciences	<i>Thousands</i>
6/1/2009	University of Nevada, Las Vegas	20
6/5/2009	Virginia Commonwealth University	22,500 (Test)
6/8/2009	Ohio State University	350
6/12/2009	Oregon Health & Science University	1,000
6/12/2009	Kirkwood Community College	1,600

6/17/2009	University of North Dakota	84,000
6/23/2009	Cornell University	45,277
6/26/2009	University of Central Missouri	7,000
7/17/2009	University of California, San Diego	30,000
7/28/2009	University of Colorado at Colorado Springs	766
8/2/2009	University of Oregon	20
8/11/2009	University of California, Berkeley	493
8/13/2009	Louisiana State University	<i>Unknown</i>
8/15/2009	Northern Kentucky University	200
8/18/2009	California State University, Los Angeles	600
8/20/2009	Boston University	6,675
8/21/2009	University of Massachusetts, Amherst	<i>Unknown</i>
8/31/2009	Bluegrass Community and Technical College	100
9/14/2009	University of Florida	34
9/24/2009	Eastern Kentucky University	5,045
9/24/2009	University of North Carolina, Chapel Hill	160,000
9/29/2009	Memorial University of Newfoundland	<i>Unknown</i>
10/3/2009	Williams College	750
10/4/2009	Suffolk Community College	300
10/12/2009	Roane State Community College	10,941
10/12/2009	University of Wisconsin, Madison	3,000
10/14/2009	California State University, Los Angeles	85
11/1/2009	Bloomsburg University of Pennsylvania	574
11/6/2009	Chaminade University	4,500
11/15/2009	California State Polytechnic University, Pomona	355
11/20/2009	Notre Dame	24,000
11/24/2009	University College Dublin	2
11/30/2009	Pennsylvania State University	303
12/4/2009	University of Nebraska Lincoln	4,000
12/4/2009	Eastern Illinois University	9,000
12/11/2009	Valdosta State University	<i>Unknown</i>
12/15/2009	University of California, San Francisco	600

12/17/2009	Alamance Community College, Beaufort County Community College, Bladen Community College, Blue Ridge Community College, Brunswick Community College, Central Carolina Community College, College of The Albemarle, Gaston College, Halifax Community College, Haywood Community College, Johnston Community College, Lenoir Community College, Martin Community College, Nash Community College, Pamlico Community College, Piedmont Community College, Richmond Community College, Roanoke-Chowan Community College, Rowan-Cabarrus Community College, Sandhills Community College, Southwestern Community College, Tri-County Community College, Vance-Granville Community College, Wake Tech Community College, Wilson Community College	51,000
12/18/2009	Pennsylvania State University	30,000
12/22/2009	Western Michigan University	<i>Unknown</i>
12/31/2009	Eastern Washington University	130,000
	Total	1,063,493²²

²² Total number of Personally Identifiable records exposed includes 11 incidents where the total number of records exposed was not reported

TYPE OF INFORMATION – SOCIAL SECURITY NUMBER

Social Security Numbers (or the non-US equivalent) ranked as the second most common type of exposed during information security incidents at colleges and universities as reported in the news. Overall, 63 incidents exposed 1,028,350 records containing Social Security numbers or the government identification numbers of a non-US country including nine 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 2009.

Table 16: Chronological List of Incidents Exposing Social Security Number Records

Date	Institution	Number Affected
1/5/2009	Clemson University	<i>Unknown</i>
1/11/2009	University of Rochester	450
1/13/2009	University of Oregon	<i>Unknown</i>
1/20/2009	University of Florida	101
1/21/2009	Missouri State University	565
1/30/2009	Kansas State University	45
2/4/2009	Ball State University	19
2/9/2009	Purdue University	962
2/14/2009	University of Alabama	37,000
2/17/2009	Broome Community College	14,000
2/19/2009	University of Florida	97,000
2/20/2009	Del Mar College	53
2/23/2009	Ryerson University	588
3/3/2009	Western Oklahoma State College	1,500
3/16/2009	University of Toledo	24,450
3/17/2009	Pennsylvania State University	1,000
3/18/2009	University of West Georgia	1,300
3/18/2009	Huron University College	25,000
3/21/2009	Solano Community College	<i>Unknown</i>
3/31/2009	Owensboro Community and Technical College	3,000
4/1/2009	Massey University	200
4/1/2009	University of Washington	6,000
4/9/2009	Pennsylvania State University, The Behrend College	10,868
5/4/2009	Kapiolani Community College	15,487
5/8/2009	University of California, Berkeley	160,000
5/30/2009	University of Arkansas for Medical Sciences	<i>Thousands</i>
6/5/2009	Virginia Commonwealth University	17,214 (SSN)
6/8/2009	Ohio State University	350
6/12/2009	Kirkwood Community College	1,600
6/17/2009	University of North Dakota	84,000
6/23/2009	Cornell University	45,277
6/26/2009	University of Central Missouri	7,000
7/17/2009	University of California, San Diego	30,000
7/28/2009	University of Colorado at Colorado Springs	766
8/11/2009	University of California, Berkeley	493
8/13/2009	Louisiana State University	<i>Unknown</i>
8/15/2009	Northern Kentucky University	200
8/18/2009	California State University, Los Angeles	600

8/20/2009	Boston University	6,675
8/21/2009	University of Massachusetts, Amherst	<i>Unknown</i>
8/31/2009	Bluegrass Community and Technical College	100
9/14/2009	University of Florida	34
9/24/2009	Eastern Kentucky University	5,045
9/24/2009	University of North Carolina, Chapel Hill	160,000
9/29/2009	Memorial University of Newfoundland	<i>Unknown</i>
10/3/2009	Williams College	750
10/4/2009	Suffolk Community College	300
10/12/2009	Roane State Community College	10,941
10/12/2009	University of Wisconsin, Madison	3,000
10/14/2009	California State University, Los Angeles	85
11/1/2009	Bloomsburg University of Pennsylvania	574
11/6/2009	Chaminade University	4,500
11/15/2009	California State Polytechnic University, Pomona	355
11/20/2009	Notre Dame	24,000
11/30/2009	Pennsylvania State University	303
12/4/2009	University of Nebraska Lincoln	4,000
12/4/2009	Eastern Illinois University	9,000
12/11/2009	Valdosta State University	<i>Unknown</i>
12/15/2009	University of California, San Francisco	600
12/17/2009	Alamance Community College, Beaufort County Community College, Bladen Community College, Blue Ridge Community College, Brunswick Community College, Central Carolina Community College, College of The Albemarle, Gaston College, Halifax Community College, Haywood Community College, Johnston Community College, Lenoir Community College, Martin Community College, Nash Community College, Pamlico Community College, Piedmont Community College, Richmond Community College, Roanoke-Chowan Community College, Rowan-Cabarrus Community College, Sandhills Community College, Southwestern Community College, Tri-County Community College, Vance-Granville Community College, Wake Tech Community College, Wilson Community College	51,000
12/18/2009	Pennsylvania State University	30,000

12/22/2009	Western Michigan University	<i>Unknown</i>
12/31/2009	Eastern Washington University	130,000
	Total	1,028,350²³

²³ Total number of Social Security Number records exposed includes nine incidents where the total number of records exposed was not reported

TYPE OF INFORMATION – USERNAMES AND PASSWORDS

Username and Password information tied as the least common type of information exposed during information security incidents at colleges and universities as reported in the news. Overall, four incidents exposed 17 records containing usernames and passwords for university computer and network systems including two incidents where the number affected was not reported. Below is a chronological list of all incidents exposing Usernames and Passwords that occurred during 2009.

Date	Institution	Number Affected
3/2/2009	University of Massachusetts	16
3/26/2009	Abilene Christian University	<i>Unknown</i>
11/19/2009	University of East Anglia	<i>Unknown</i>
12/11/2009	Daytona State College	1
	Total	17²⁴

²⁴ Total number of Username and Password records exposed includes two incidents where the total number of records exposed was not reported

INSTITUTIONS AFFECTED

During 2009, 102 different information security incidents occurred at 86 different colleges and universities. Below is an alphabetical list of all 102 colleges and universities.

Table 17: Alphabetical List of Institutions

Institutions
Abilene Christian University
Alamance Community College
Ball State University
Beaufort County Community College
Bladen Community College
Bloomsburg University of Pennsylvania
Blue Ridge Community College
Bluegrass Community and Technical College
Boston University
Brigham Young University
Broome Community College
Brunswick Community College
California State Polytechnic University, Pomona
California State University, Los Angeles
Central Carolina Community College
Chaminade University
Clemson University
College of The Albemarle
Cornell University
Daytona State College
Del Mar College
Drake University
Eastern Illinois University
Eastern Kentucky University
Eastern Washington University
Gaston College
Halifax Community College
Haywood Community College
Huron University College
Johns Hopkins University
Johnston Community College
Kansas State University
Kansas University
Kapiolani Community College
Kirkwood Community College
Lenoir Community College
Louisiana State University
Martin Community College
Massey University
Memorial University of Newfoundland
Missouri State University

Nash Community College
National University of Singapore
Northern Kentucky University
Notre Dame
Ohio State University
Oregon Health & Science University
Oregon University System
Owensboro Community and Technical College
Pacific University
Pamlico Community College
Pennsylvania State University
Pennsylvania State University, The Behrend College
Piedmont Community College
Purdue University
Richmond Community College
Roane State Community College
Roanoke-Chowan Community College
Rowan-Cabarrus Community College
Ryerson University
Sandhills Community College
Solano Community College
Southwestern Community College
Southwestern Oregon Community College
Suffolk Community College
Texas Woman's University
Trent University
Tri-County Community College
Tufts University
University College Dublin
University of Alabama
University of Arkansas for Medical Sciences
University of California, Berkeley
University of California, San Diego
University of California, San Francisco
University of Central Missouri
University of Colorado at Colorado Springs
University of Colorado, Denver
University of East Anglia
University of Florida
University of Massachusetts
University of Massachusetts, Amherst
University of Nebraska Lincoln
University of Nevada, Las Vegas
University of North Carolina, Chapel Hill
University of North Dakota
University of Oregon
University of Rochester
University of Texas, Brownsville
University of Toledo
University of Vermont

University of Washington
University of West Georgia
University of Wisconsin, Madison
Valdosta State University
Vance-Granville Community College
Virginia Commonwealth University
Wake Tech Community College
Western Michigan University
Western Oklahoma State College
Williams College
Wilson Community College

PART 4: EDUCATIONAL SECURITY INCIDENTS

The fourth and final part of the ESI Year in Review – 2009 is a collection of all of the educational security incidents that appear on the ESI web site for 2009. 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 addresses 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 possible that the links below are still valid; there have been no attempts by ESI or the author to verify this fact.

FORMER CLEMSON OFFICIAL ALLEGES UNIVERSITY SOLD COMPUTERS CONTAINING PRIVATE DATA

Quick Facts

- Date: 1/5/2009
- Institution: [Clemson University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: *Unknown*
- Source: [DataBreaches.net](#) [2]
- Abstract source: [Greenville Online](#) [3]

Abstract

A former Clemson University official is alleging that the university sold surplus computers containing protected data without erasing the hard drives. According to Clemson University, a 2007 audit did find surplus computers meant for resale did contain personal information. However, these computers were not sold once the audit found the data according to Clemson spokesperson Cathy Sims. The university has purchased a hard drive shredder for all hard drives in surplus computers.

Links:

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

[2] <http://www.databreaches.net/?p=253>

[3] <http://www.greenvilleonline.com/article/20090105/NEWS01/90105023/1069/YOURUPSTATE01>

OVER 400 SOCIAL SECURITY NUMBERS STOLEN FROM UNIVERSITY OF ROCHESTER DATABASE

Quick Facts

- Date: 1/11/2009
- Institution: [University of Rochester](#) [1]
- Type of Incident: Penetration
- Number Affected: 450
- Source: [OSF Data Loss Database](#) [2]
- Abstract Source: [University of Rochester News Release](#) [3]

Abstract

The University of Rochester announced that it has discovered the unauthorized copying of approximately 450 Social Security numbers from a non-academic database. The university is alerting current and former students affected by the incident through email and postal mail. Officials notified the authorities after discovering the breach including the FBI, the NY Attorney General and the NYS Office of Cyber Security. All affected individuals are being offered one year of credit monitoring at no cost.

Update 1/20/09 Corrected typo in title and fixed the abstract link. Special thanks to Allison Dolan for making us aware of these problems - Adam

Links:

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

[2] <http://datalossdb.org/incidents/1448-personal-information-including-social-security-numbers-of-about-450-in-hacked-database>

[3] <http://www.rochester.edu/news/show.php?id=3298>

UNIVERSITY OF OREGON LAPTOP CONTAINING PERSONAL INFORMATION STOLEN

Quick Facts

- Date: 1/13/2009
- Institution: [University of Oregon](#) [1]
- Type of Incident: Theft
- Number Affected: *Unknown*
- Source: [ESI](#) [2]
- Abstract Source: [University of Oregon Media Relations](#) [3]

Abstract

The University of Oregon announced that an employee's laptop containing Youth Transition Program (YTP) participant information was stolen. The laptop contained the names and Social Security numbers of YTP participants from 2004 to 2007. Youth Transition Program is a program that services more than 1,200 individuals between 17 and 21 with disabilities and provides career planning and employment services. The laptop was password protected, but there was no mention of encryption. University of Oregon provides evaluation services for YTP to help determine which programs are most effective. The university sent out notification letters to affected individuals and urged these individuals to monitor their credit scores.

Links:

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

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

[3] <http://pmr.uoregon.edu/current-uo-news/archive/2009/january/stolen-computer-contains-participants2019-personal-information/>

HUNDREDS AT RISK AFTER SOUTHWESTERN OREGON COMMUNITY COLLEGE LAPTOP THEFT

Quick Facts

- Date: 1/16/2009
- Institution: [Southwestern Oregon Community College](#) [1]
- Type of Incident: Theft
- Number Affected: 200
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [KCBY](#) [3]

Abstract

Southwestern Oregon Community College is alerting students after a laptop containing personal information was stolen. The laptop contained the student records of approximately 200 students. The college has also placed a privacy hold on the affected SOCC records. There is no information if the college will offer free credit monitoring to any of the affected individuals or what information was contained on the laptop.

Links:

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

[2] <http://www.databreaches.net/?p=730>

[3] <http://www.kcby.com/news/local/37748899.html>

LDAP CONFIGURATION ERROR PUTS SOCIAL SECURITY NUMBERS AT RISK

Quick Facts

- Date: 1/20/2009
- Institution: [University of Florida](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 101
- Source: [ESI](#) [2]
- source: [University of Florida Privacy Office](#) [3]

Abstract

The University of Florida announced that it has discovered an error in its LDAP system that potentially exposed private information. The error allowed outside access to the LDAP directory which contained Social Security numbers, used as student identifiers prior to 2003. An investigation into the error discovered the outside access was enabled an accident four months ago. The investigation did find queries that could have returned the user IDs and Social security numbers of 101 individuals. UF staff immediately removed the Social Security numbers from the LDAP directory. The University of Florida has also set up a web site - privacy.ufl.edu/incidents/2009/ldap/answers.html [4] - with more information on the incident.

Links:

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

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

[3] <http://privacy.ufl.edu/incidents/2009/ldap/>

[4] <http://privacy.ufl.edu/incidents/2009/ldap/answers.html>

EMAIL ATTACHMENT EXPOSES MISSOURI STATE UNIVERSITY FOREIGN STUDENT INFORMATION

Quick Facts

- Date: 1/21/2009
- Institution: [Missouri State University](http://www.missouristate.edu) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 565
- Source: [ESI](http://www.adamdodge.com/esi) [2]
- Abstract Source: [News-Leader](http://www.news-leader.com/article/20090121/NEWS04/901210456) [3]

Abstract

Missouri State University is working to contact foreign students after an email was accidentally sent out containing personal information. The email in question was sent out with a spreadsheet attachment containing the names and Social Security numbers and other sensitive information of 565 foreign students enrolled at MSU. The email was sent out to 179 students on January 14 by the directory of international student services. On January 16, another email was sent out asking these students to please delete the email with the attachment. MSU officials hope that the risks are lower since not all of the students had Social Security numbers. However, MSU is currently looking at the feasibility of obtaining insurance for the affected students.

Links:

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

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

[3] <http://www.news-leader.com/article/20090121/NEWS04/901210456>

K-STATE FINDS STUDENT INFORMATION ONLINE SINCE 2001

Quick Facts

- Date: 1/30/2009
- Institution: [Kansas State University](http://www.k-state.edu) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 45
- Source: [ESI](http://www.adamdodge.com/esi) [2]
- Abstract Source: [TradingMarkets.com](http://www.tradingmarkets.com/site/news/Stock_News/2151408/) [3]

Abstract

Kansas State University is working to notify students after it discovered personal information had been available online. The information, available online since 2001, contained in the names, grades and Social Security numbers of 45 student enrolled in the Spring 2001 AGEC 490 "Computer Applications in Agricultural Economics and Agribusiness" course. In the notification letter, K-State officials urge the affected students to take steps to protect their identities. The university has begun to take steps to prevent similar incidents from occurring in the future.

Links:

[1] <http://www.k-state.edu>

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

[3] [http://www.tradingmarkets.com/site/news/Stock News/2151408/](http://www.tradingmarkets.com/site/news/Stock_News/2151408/)

EMAIL LEAKS BALL STATE EMPLOYEE SOCIAL SECURITY NUMBERS

Quick Facts

- Date: 2/4/09
- Institution: [Ball State University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 19
- Source: [ESI](#) [2]
- Abstract Source: [Ball State Daily News Online](#) [3]

Abstract

Ball State University announced that an email sent to special event employees contained personal information. The email, sent to 91 employees to verify information, contained the Social Security numbers of 19 special event employees. According to the Ball State Associate VP for Marketing and Communications Tony Proudfoot, the Social Security numbers were accidentally entered into the Employee ID field by the employees themselves. The university became aware of the problem within minutes of sending the email as employees began contacting the university. Once notified, Ball State employees went to work requesting email recipients delete the email and contacting the 19 affected individuals to offer to cover any identity theft expenses suffered by the individuals.

Links:

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

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

[3]

<http://media.www.bsudailynews.com/media/storage/paper849/news/2009/02/04/News/Social.Security.Numbers.Leaked-3611556.shtml>

DRAKE UNIVERSITY ACADEMIC RECORDS INADVERTENTLY RELEASED

Quick Facts

- Date: 2/9/2009
- Institution: [Drake University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 800
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [The Times-Delphic](#) [3]

Abstract

Drake University announced that an email sent to the sorority and fraternity house presidents accidentally contained student grade information. The two emails, one to fraternity house presidents and the other to sorority house presidents, contained the grades for all fraternity members and sorority members respectively. In all, 800 students were affected by these emails. The emails were intended for the fraternity and sorority chapter presidents, but were sent to the wrong list. The university sent a second email to all house presidents asking them to delete the email immediately. In addition, the university with fraternity and sorority presidents requiring each of them to sign a form indicating the email and attachment had been deleted.

Links:

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

[2] <http://www.databreaches.net/?p=1301>

[3]

<http://media.www.timesdelphic.com/media/storage/paper1086/news/2009/02/05/News/Academic.Records.Inadvertently.Released-3613357.shtml>

BREACHED TRENT UNIVERSITY SERVER CONTAINED PERSONAL INFORMATION

Quick Facts

- Date: 2/9/2009
- Institution: [Trent University](#) [1]
- Type of Incident: Penetration
- Number Affected: 21
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [The Peterborough Examiner](#) [3]

Abstract

Trent University is alerting donors and alumni after it discovered a server containing personal information had been breached. The server, housed off site, contained donor and alumni information including names, employers, job titles, degree information and 21 credit card numbers. According to Trent University VP of External Relations, the server was breached after a firewall failed following a power surge. An investigation into the incident showed that the unknown individual responsible for the breach was trying to repurpose the server to host music or video files. According to Lister, the breach has cost the university \$20,000 and Trent officials are considering suing the external hosting company.

Thank you to ESI reader Mike Patterson for making us aware of this incident. - Adam

Links:

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

[2] <http://www.databreaches.net/?p=1315>

[3] <http://www.thepeterboroughexaminer.com/ArticleDisplay.aspx?e=1421154>

MISTAKE SENDS PURDUE 1099 FORMS TO WRONG INDIVIDUALS

Quick Facts

- Date: 2/9/2009
- Institution: [Purdue University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 962
- Source: [ESI](#) [2]
- Abstract Source: [The Exponent Online](#) [3]

Abstract

Purdue University began notifying individuals and businesses after it discovered a mistake was made when sending out 1099 tax forms. The forms were printed two per page with a perforation in between and were meant to be separated prior to mailing. However, the forms were not separated and, as a result, several individuals received two 1099 forms, a correct form and one belonging to someone else. In all 962 individuals and 248 businesses had their personal information such as names, Social Security numbers and financial information shared with others. The university acted quickly to contact the affected individuals and has setup a Web site - news.uns.purdue.edu/Payroll0901.html [4] - to help answer questions about the incident.

Links:

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

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

[3] http://www.purdueexponent.org/index.php?module=article&story_id=14823

[4] <http://news.uns.purdue.edu/Payroll0901.html>

SEVENTEEN SERVERS BREACHED AT UNIVERSITY OF ALABAMA

Quick Facts

- Date: 2/14/2009
- Institution: [University of Alabama](#) [1]
- Type of Incident: Penetration
- Number Affected: 37,000
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [TuscaloosaNews.com](#) [3]

Abstract

The University of Alabama recently announced that it had discovered a number of servers had been breached by an unknown individual. In total, 17 servers were illegally accessed in November. According to UA Vice Provost of Information Technology John McGowan none of the servers contained student or medical records. However, the computers did contain the names, address and Social Security numbers of 37,000 individuals who had blood or urine lab work going back to 1994. In a letter sent Friday, University of Alabama urges affected individuals to place fraud alerts on credit files and monitor credit reports. According to a forensic investigation, the intruder was not in the system long enough to retrieve any sensitive data.

Links:

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

[2] <http://www.databreaches.net/?p=1502>

[3]

http://www.tuscaloosanews.com/article/20090214/NEWS/902130209/1007?Title=UA_says_probe_continues_of_08_hacking

BCC ALUMNI MAGAZINE COVERS CONTAIN SOCIAL SECURITY NUMBERS

Quick Facts

- Date: 2/17/2009
- Institution: [Broome Community College](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 14,000
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [PressConnects](#) [3]

Abstract

Broome Community College is working to change processes after alumni Social Security numbers ended up on the cover of a recent mailing. BCC believe that less than 14,000 of the 28,000 winter/spring 2009 alumni magazine has Social Security numbers on the cover. According to BCC Social Security numbers were used until 2004 as student identification numbers and the old student ID numbers were used to verify address. BCC alumni office spokesperson Rich David said that the vendor that printed the magazine destroyed the list with Social Security numbers in front of witnesses.

Links:

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

[2] <http://www.databreaches.net/?p=1577>

[3] <http://www.pressconnects.com/article/20090217/NEWS01/902170341>

UNIVERSITY OF FLORIDA BREACH POTENTIALLY EXPOSES INFORMATION OF 97,000 INDIVIDUALS

Quick Facts

- Date: 2/19/2009
- Institution: [University of Florida](#) [1]
- Type of Incident: Penetration
- Number Affected: 97,200
- Source: [ESI](#) [2]
- Abstract Source: [University of Florida News](#) [3]

Abstract

The University of Florida is working to notify current and past students, faculty and staff after staff discovered a server breach. The "Grove" server hosted course documentation and course documentation containing files with the names and Social Security numbers of up to 97,200 individuals. UF staff discovered the breach on Jan 14 during routine IT system review. The computer was shut down and the UF launched an investigation. While the investigation was able to confirm unauthorized access had occurred, staff were not able to determine if the files containing private information had been accessed. In a [letter](#) [4] (pdf) to the individuals affected by the breach, UF calls the risk of identity theft low but suggests people follow FTC guidelines. The University of Florida has created a web site - [privacy.ufl.edu/incidents/2009/academic-technology](#) [5] - with more information on the breach.

Links:

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

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

[3] <http://news.ufl.edu/2009/02/19/grove/>

[4] <http://privacy.ufl.edu/incidents/2009/academic-technology/breach-letter.pdf>

[5] <http://privacy.ufl.edu/incidents/2009/academic-technology/>

DEL MAR CLASS ROSTER WITH SOCIAL SECURITY NUMBERS STOLEN FROM CAR

Quick Facts

- Date: 2/20/2009
- Institution: [Del Mar College](#) [1]
- Type of Incident: Theft
- Number Affected: 53
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [Caller-Times](#) [3]

Abstract

Del Mar College is alerting students after a class roster containing personal information was stolen. The roster, stolen from an instructor's vehicle, contained the names and Social Security numbers of 53 students in Del Mar College's General Educational Development program. According to Del Mar College President Mark Escamilla, the college is taking steps to support the students affected by this breach. Officials met with the student and provided information on preventing identity theft and how to contact the different credit bureaus. Students were also informed to contact the police if the student noticed suspicious activity on their credit reports.

Links:

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

[2] <http://www.databreaches.net/?p=1656>

[3] http://www.caller.com/news/2009/feb/20/del_mar_roster/

SOFTWARE ERROR EXPOSES RYERSON STUDENT INFORMATION

Quick Facts

- Date: 2/23/2009
- Institution: [Ryerson University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 588
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [CNW](#) [3]

Abstract

Ryerson University is working to notify students after it became aware of an error in the University's Student Administration System (SAS) that potentially exposed student information. The error in the SAS system allowed individuals using SAS to view others' personal information including names, genders, dates of birth, student numbers, mailing addresses, email addresses, and Social Insurance numbers. Ryerson became aware of the error when three students notified the university in late December and early January. Ryerson installed a software patch on January 9th to fix the problem and hired Ernst & Young to investigate the vulnerability. The investigation determined that as many as 366 students had access to the personal information of others and that the patch installed fixed the vulnerability. Ryerson University President Sheldon Levy has commended the three students that alerted the university to the error for their initiative, integrity and sense of responsibility.

Links:

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

[2] <http://www.databreaches.net/?p=1726>

[3] <http://www.newswire.ca/en/releases/archive/February2009/23/c2869.html>

POLICE ALLEGE FORMER IT ADMIN STOLE NUDE FACEBOOK PICTURES

Quick Facts

- Date: 3/2/2009
- Institution: [University of Massachusetts](#) [1]
- Type of Incident: Employee Fraud
- Number Affected: 16
- Source: [Pogo Was Right](#) [2]
- Abstract Source: [The Register](#) [3]

Abstract

A former University of Massachusetts IT administrator is facing charges that he illegally accessed 16 student Facebook accounts and stole nude photos. Robert J DeCampos Jr faces 13 misdemeanor counts of unauthorized computer access and one felony count of larceny. According to court documents, DeCampos used student email accounts to gain access to the Facebook accounts where he was able to download the nude photos these accounts contained. DeCampos was fired by the university on October 20, four days after the discovery of the alleged computer trespass.

Links:

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

[2] <http://www.pogowasright.org/article.php?story=20090301102307640>

[3] http://www.theregister.co.uk/2009/02/27/admin_steals_nude_facebook_pics/

LIBRARY PATRON DATA AT RISK AFTER SEVER BREACH

Quick Facts

- Date: 3/3/2009
- Institution: [Western Oklahoma State College](#) [1]
- Type of Incident: Penetration
- Number Affected: 1,500
- Source: [ESI](#) [2]
- Abstract Source: [The Oklahoman](#) [3]

Abstract

Western Oklahoma State College is alerting staff and students after a breach potentially exposed personal information. On February 18, the college discovered that a server, containing library patron data, had been breached sometime in November and a rootkit had been installed. The unauthorized access potentially exposed the names, Social Security numbers and other personal information on 1,500 campus library users going back to 2004. Western Oklahoma State College does not believe the personal information was accessed but officials urged patrons to monitor their credit reports. The college has created a web site - [incident.wosc.edu](#) [4] - and a hot line - 580-477-7992 - to help answer questions about this breach.

Links:

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

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

[3] <http://newsok.com/credit-monitoring-urged-after-breach/article/3349979>

[4] <http://incident.wosc.edu>

STOLEN UNIVERSITY OF TOLEDO COMPUTER CONTAINS STUDENT AND FACULTY INFORMATION

Quick Facts

- Date: 3/16/2009
- Institution: [University of Toledo](http://www.utoledo.edu) [1]
- Type of Incident: Theft
- Number Affected: 24,450
- Source: [DataBreaches.net](http://www.databreaches.net) [2]
- Abstract Source: [Toledo Blade](http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20090316/NEWS04/903160231) [3]

Abstract

The University of Toledo is working to notify faculty and students after a computer containing personal information was discovered stolen. The computer contained directory and educational information on 24,000 university students as well as the names, Social Security numbers, and dates of birth of 450 faculty members. The computer was stolen out of a locked office that was pried open by the thief. According to university officials, the computer was password protected and several files on the computer were individually encrypted or had additional password protection.

Links:

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

[2] <http://www.databreaches.net/?p=2405>

[3] <http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20090316/NEWS04/903160231>

VIRUS PROMPTS PENN STATE BREACH NOTIFICATION

Quick Facts

- Date: 3/17/2009
- Institution: [Penn State University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 1,000
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [Centre Daily Times](#) [3]

Abstract

Penn State University is working to alert employees after a virus infection may have exposed personal information. The infected computer, located in the Penn State Office of Physical Plant, was found to contain the names and Social Security numbers of about 1,000 employees from 2000. Penn State discontinued the use of Social Security numbers in 2005, but legacy files still contain this information according to Physical Plant spokesperson Paul Ruskin. The Office of Physical Plant has alerted all affected individuals and is reviewing all old data for the use of Social Security numbers.

Links:

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

[2] <http://www.databreaches.net/?p=2437>

[3] <http://www.centredaily.com/news/local/story/1177404.html>

UNIVERSITY NOTIFIES STUDENTS, FACULTY OVER SUMMER LAPTOP THEFT

Quick Facts

- Date: 3/18/2009
- Institution: [University of West Georgia](http://www.westga.edu) [1]
- Type of Incident: Theft
- Number Affected: 1,300
- Source: [OSF Data Loss Database](http://datalossdb.org) [2]
- Abstract Source: [Fort Mill Times](http://www.fortmilltimes.com) [3]

Abstract

University of West Georgia officials are alerting faculty and students after it discovered that a stolen laptop contained personal information. The laptop, stolen from a professor vacationing in Italy during the summer, contained the names, addresses, phone numbers and Social Security numbers of 1,300 students and faculty. The reason for the delayed notification, according to university officials, was that the university was not aware the laptop contained any sensitive information until recently.

Links:

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

[2] <http://datalossdb.org/incidents/1839-stolen-laptop-exposes-1300-student-and-faculty-names-addresses-and-social-security-numbers>

[3] <http://www.fortmilltimes.com/124/story/496932.html>

HURON STAFF WORKING TO NOTIFY CURRENT, FORMER STUDENTS AFTER SERVER BREACH

Quick Facts

- Date: 3/18/2009
- Institution: [Huron University College](http://www.huronuc.ca/) [1]
- Type of Incident: Penetration
- Number Affected: 25,000
- Source: [ESI](http://www.adamdodge.com/esi) [2]
- Abstract Source: [Western News](http://communications.uwo.ca/com/western_news/stories/huron_university_college_data_exposure_20090318443874/) [3]

Abstract

Huron University College is looking for help in contacting former students, applicants and residence after a server containing personal information was found to have been breached by an unknown party. The breach, discovered by staff attempting to fix another problem, potentially exposed the names, SIN numbers and dates of birth of some 25,000 individuals including those students residing on campus between 1999 and present, college applicants between 1992 and 2008, and register students between 2004 and present. While the investigation into the incident has not found any evidence that the personal information was accessed, the college cannot rule that out. Huron has created a hotline - 866-953-7745 - to help address any concerns or questions about this incident.

Links:

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

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

[3]

http://communications.uwo.ca/com/western_news/stories/huron_university_college_data_exposure_20090318443874/

SECURITY INCIDENT PROMPTS SHREDDING CHANGE AT SCC

Quick Facts

- Date: 3/21/2009
- Institution: [Solano Community College](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: *Unknown*
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [The Reporter](#) [3]

Abstract

Solano Community College is working to change its shredding policies after a mistake almost exposed student information. Solano staff discovered that a report containing the names, addresses, and Social Security numbers of the 2008 graduating class accidentally ended up as scrap paper in a mathematics lab. Staff were able to collect all pages of the report before any of it was used by students. According to Solano Community College Vice President of Technology and Learning Resources that the college has steps to tighten the security of printed documents to help avoid this type of mistake in the future. Solano has notified all affected graduates and has setup a hotline - 707-863-7102 - to help answer questions about the incident.

Links:

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

[2] <http://www.databreaches.net/?p=2540>

[3] http://www.thereporter.com/news/ci_11965958

ABILENE CHRISTIAN UNIVERSITY SERVER BREACHED

Quick Facts

- Date: 3/26/2009
- Institution: [Abilene Christian University](#) [1]
- Type of Incident: Penetration
- Number Affected: *Unknown*
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [ReporterNews.com](#) [3]

Abstract

Abilene Christian University sent out an email informing the campus community about a breach of one the ACU's computer servers. The breached system contained a database of usernames and passwords tied to the ACU's email system. According to the university, this incident appears to be the action of a single individual and there is no evidence that the intruder obtained any personal information. Kevin Roberts, associate vice president of operations with the university, the university knows the identity of the individual responsible for the breach, but is not releasing any additional information because the ongoing investigation.

Links:

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

[2] <http://www.databreaches.net/?p=2653>

[3] <http://www.reporternews.com/news/2009/mar/26/acu-says-computer-server-hacked/>

PACIFIC UNIVERSITY LAPTOP CONTAINING SENSITIVE INFORMATION MISSING

Quick Facts

- Date: 3/28/2009
- Institution: [Pacific University](#) [1]
- Type of Incident: Theft
- Number Affected: *Unknown*
- Source: [ESI](#) [2]
- Abstract Source: [KPTV](#) [3]

Abstract

Pacific University announced on Friday that administrators are trying to locate a stolen laptop that may contain sensitive information. The laptop, stolen from a staff member's home, did not contain any Social Security numbers. However, the university could not rule out other types of sensitive information. Administrators are encouraging staff and students to monitor their personal information and accounts even though there has been no evidence of misuse. Pacific has setup a web site - www.pacificu.edu/alerts/identity.cfm - to help answer questions about this incident.

Links:

- [1] <http://www.pacificu.edu>
- [2] <http://www.adamdodge.com/esi>
- [3] <http://www.kptv.com/education/19035439/detail.html>

OWENSBORO COMMUNITY AND TECHNICAL COLLEGE MISSING HARD DRIVE CONTAINS STUDENT INFORMATION

Quick Facts

- Date: 3/31/2009
- Institution: [Owensboro Community and Technical College](#) [1]
- Type of Incident: Theft
- Number Affected: 3,000
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [WFIE](#) [3]

Abstract

Owensboro Community and Technical College is alerting students after the theft of a hard drive containing sensitive information. The hard drive contained the names, Social Security numbers, and student ID numbers of 3,000 Owensboro students. Owensboro staff has filed a police report about the missing hard drive.

Links:

[1] <http://www.octc.kctcs.edu/Default.htm>

[2] <http://www.databreaches.net/?p=2719>

[3] <http://www.14wfie.com/Global/story.asp?S=10106602&nav=3w6o>

MASSEY UNIVERSITY ERROR ALLOWS STUDENTS TO ACCESS PERSONAL INFORMATION OF OTHERS

Quick Facts

- Date: 4/1/2009
- Institution: [Massey University](http://www.massey.ac.nz/) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 200
- Source: [OSF Data Loss Database](http://datalossdb.org/) [2]
- Abstract Source: [Otago Daily Times](http://www.odt.co.nz/) [3]

Abstract

An error in Massey University's MyMassey intranet system allowed students to access the personal information of others. The error, discovered by Rawa Karetai, allowed access to the Massey identification numbers, full names, dates of birth, IRD numbers, academic transcripts, contact addresses and phone numbers of almost 200 Massey students. Karetai discovered the error at 10:40PM and reported it to the university's security office. According to Massey CIO Gerrit Bahlman, the error was caused by an operating system patch release. The MyMassey system was taken offline by 1:42AM to allow the university to fix the flaw.

Links:

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

[2] <http://datalossdb.org/incidents/1858-students-details-including-names-addresses-ird-numbers-exposed-on-intranet>

[3] <http://www.odt.co.nz/news/national/49970/system-fault-makes-student-information-public>

UNIVERSITY OF WASHINGTON BREACHES EXPOSES WORKER INFORMATION

Quick Facts

- Date: 4/1/2009
- Institution: [University of Washington](#) [1]
- Type of Incident: Penetration
- Number Affected: 6,000
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [The Seattle Times](#) [3]

Abstract

The University of Washington sent out notifications to workers after two server breaches may have exposed personal information. The servers, part of the university parking-management system, contain the names and Social Security numbers of 6,000 workers. The university became aware of a problem on December 30th when a police report states that the computers were showing obvious signs of compromise starting around December 6th. According to the university's CISO Kirk Bailey, it took the university until the end of February or the beginning of March to complete the investigation, which included a "full-blown computer forensic investigation".

Links:

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

[2] <http://www.databreaches.net/?p=2809>

[3] http://seattletimes.nwsourc.com/html/localnews/2008958501_uwdata01m.html

BRIGHAM YOUNG UNIVERSITY EMAIL ERROR SENDS STUDENT IDS AND GPAS TO ALL STUDENTS

Quick Facts

- Date: 4/2/2009
- Institution: [Brigham Young University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: *Unknown*
- Source: [ESI](#) [2]
- Abstract Source: [Wired Campus - The Chronicle of Higher Education](#) [3]

Abstract

Brigham Young University officials are working to calm student fears after an email message containing student information was sent to the wrong recipients. The email in question, accidentally sent to all students in the College of Humanities instead of BYU's Registrar, contained the student IDs and GPAs of all students in the College of Humanities. While the email does not expose the students affected to identity theft, students have been urged to delete the message immediately.

Special thank you to Allison Dolan for making ESI aware of this incident - Adam

Links:

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

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

[3] http://chronicle.com/wiredcampus/article/3691/e-mail-goof-at-brigham-young-u-makes-student-gpas-and-ids-public?utm_source=at&utm_medium=en

POTENTIAL BREACH AT PENN STATE BEHREND

Quick Facts

- Date: 4/9/2009
- Institution: [Penn State University - Erie, The Behrend College](#) [1]
- Type of Incident: Penetration
- Number Affected: 10,868
- Source: [OSF Data Loss Database](#) [2]
- Abstract Source: [Penn State Live](#) [3]

Abstract

Penn State University officials are working to notify individuals after a computer containing personal information may have been breached. The server, containing historical information, contained the names and Social Security numbers of 10,868 individuals at Erie, PA Behrend campus. Behrend staff became aware of the potential breach when the college's intrusion detection system alerted them of the problem. Staff investigated the incident and confirmed the computer contained Social Security numbers. However, staff was not able to confirm that the personal information was affected by the breach. The computer was taken offline and the sensitive data was removed. Behrend will begin sending out notification letters to the affected individuals April 11th.

Links:

[1] <http://www.erie.psu.edu>

[2] <http://datalossdb.org/incidents/1881-10-868-social-security-numbers-open-for-potential-breach>

[3] <http://live.psu.edu/story/39025>

NATIONAL UNIVERSITY OF SINGAPORE EMAIL LEAKS ALUMNI DATA

Quick Facts

- Date: 4/20/2009
- Institution: [National University of Singapore](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 15,794
- Source: [ESI](#) [2]
- Abstract Source: [Asia One](#) [3]

Abstract

The National University of Singapore is reassessing its information security policies after an email sent to 450 individuals accidentally contained alumni information. The email, sent by the NUS Career Center to a number of alumni, contained a file that had name, home address, subject major and phone number information 15,794 NUS alumni. This incident involves alumni that have graduated from NUS from 1993 through last year. The staff member was using an old email as a template and forgot to remove the file before sending. NSU is implementing new security controls such as requiring at least two staff members to review emails to stakeholder groups, password-protecting database access and restricting how passwords are distributed.

Links:

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

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

[3] <http://www.asiaone.com/News/Education/Story/A1Story20090419-136168.html>

TWU DEGREE AUDITING SYSTEM ERROR EXPOSES STUDENT COURSE, GRADES

Quick Fact

- Date: 4/25/2009
- Institution: [Texas Woman's University](http://www.twu.edu) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 12,000
- Source: [ESI](http://www.esi.com) [2]
- Abstract Source: [Dallas News](http://www.dallasnews.com) [3]

Abstract

Texas Woman's University corrected an error in the university's degree auditing program earlier in the week. The error allowed anyone accessing the system to view the names, courses and grades of the 12,000 students enrolled at the university. The error was discovered by a TWU junior and reported to the university. According to Robert Placido, Associate Vice President of Information Technology Services, the error allowed students to access the advisor section of the Degree Audit Report System. However, this access did not allow any changes to the information. TWU staff took the system off line within four hours and the system was fixed and put back online within a day. According to Placido, out of the 36 individuals logged into the system when the error was reported, eight were unauthorized users.

Links:

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

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

[3] http://www.dallasnews.com/sharedcontent/dws/dn/education/stories/DN-twusecurity_25met.ART.State.Edition1.4aea46d.html

MALWARE INFECTS KAPIOLANI COMMUNITY COLLEGE COMPUTE WITH ACCESS TO SENSITIVE INFORMATION

Quick Facts

- Date: 5/4/2009
- Institution: [Kapiolani Community College](http://kapiolani.hawaii.edu/) [1]
- Type of Incident: Penetration
- Number Affected: 15,487
- Source: [OSF Data Loss Database](http://datalossdb.org/) [2]
- Abstract Source: [KITV](http://www.kitv.com/) [3]

Abstract

Kapiolani Community College announced that it discovered a potential breach of a computer with access to sensitive student information. On April 15, KCC staff discovered that a computer with access to a network containing names, addresses, phone numbers dates of birth and Social Security numbers was infected with malware that could allow remote access and control. The computer was involved with student financial aid applications between January 2004 and April 15, 2009. KCC is alerting 15,487 current and former students and encouraging them to monitor their credit reports

Links:

[1] <http://kapiolani.hawaii.edu/>

[2] <http://datalossdb.org/incidents/1951-malware-affects-computer-with-access-to-15-487-names-addresses-phone-numbers-dates-of-birth-and-social-security-numbers>

[3] <http://www.kitv.com/news/19367867/detail.html>

HACKERS BREACH UC BERKELEY DATABASE, STEAL SOCIAL SECURITY NUMBERS

Quick Facts

- Date: 5/08/2009
- Institution: [University of California, Berkeley](#) [1]
- Type of Incident: Penetration
- Number Affected: 160,000+
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [UC Berkeley News Update](#) [3]

Abstract

The University of California, Berkeley began notifying individuals today after staff discovered an unknown individual(s) attacked a restricted database on a computer in the university's health services center. The computer contained the names, Social Security numbers, health insurance information, immunization records, and patient physician information on more the 160,000 UC Berkeley student and alumni as well as former Mills College students. UC Berkeley discovered the breach in April and immediately took action. The affected database was taken offline and UC Berkeley contacted the both campus police and the FBI. According to Shelton Waggener, UC Berkeley's associate vice chancellor for information technology and its chief information officer, the university takes its data steward responsibilities serious and regrets the incident. UC Berkeley has created a web site - [datatheft.berkeley.edu](#) [4] - and a hotline - 888-729-3301 - to help answer additional questions about this incident.

Links:

- [1] <http://www.berkeley.edu>
- [2] <http://www.databreaches.net/?p=3821>
- [3] <http://datatheft.berkeley.edu/news.shtml>
- [4] <http://datatheft.berkeley.edu>

USER WEB SITE SECURITY FAILURE LEADS TO BALL STATE BREACH

Quick Facts

- Date: 5/22/2009
- Institution: [Ball State University](#) [1]
- Type of Incident: Penetration
- Number Affected: 2,000
- Source: [ESI](#) [2]
- Abstract Source: [Ball State Daily News Online](#) [3]

Abstract

Ball State University officials announced that the recent compromise of one of the university's iWeb servers was caused by user error and not the recently disclosed IIS vulnerability. According to officials, one of the users on the server failed to properly secure their web space which allowed an unknown individual(s) to upload a malicious script to the server. The breached server was one of eight such web servers and housed web accounts for about 2,000 individuals. Most of these 2,000 had their web content replaced with a taunting message. Ball State officials say the iWeb server was backed up a few hours before the breach and most content should be restored soon.

Links:

[1] <http://cms.bsu.edu>

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

[3]

<http://media.www.bsudailynews.com/media/storage/paper849/news/2009/05/21/Dnupdate/Update.Iweb.Breach.Resulted.From.User.Failing.To.Secure.Their.Account-3743600.shtml>

STOLEN UAMS COMPUTER CONTAINED CURRENT, FORMER EMPLOYEE INFORMATION

Quick Facts

- Date: 5/30/09
- Institution: [University of Arkansas for Medical Sciences](#) [1]
- Type of Incident: Theft
- Number Affected: *Thousands*
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [Arkansas Democrat-Gazette](#) [3]

Abstract

The University of Arkansas for Medical Sciences (UAMS) announced that it had recovered a stolen computer that contained employee personal information. The computer, stolen on May 18th by a UAMS worker, was used to create identification badges and contained the names and Social Security numbers of thousands of current and former student workers, staff members and contractors. According to UAMS officials, the individual that took the computer did not know about the personal information and that this sensitive information was protected by multiple passwords. UAMS is implementing changes that disallow the storage of sensitive information on desktop computers and will continue an existing project to deploy encryption across campus.

6/15/09 - Corrected small typo. Thanks to Allison Dolan for letting us know. - Adam

Links:

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

[2] <http://www.databreaches.net/?p=4380>

[3] <http://www.nwanews.com/adg/News/260771/>

UNLV NOTIFIES STUDENTS OVER POTENTIAL DATA LEAK

Quick Facts

- Date: 6/1/09
- Institution: [University of Nevada, Las Vegas](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 20
- Source: [ESI](#) [2]
- Abstract Source: [UNLV Rebel Yell](#) [3]

Abstract

The University of Nevada, Las Vegas College of Sciences sent notices to a handful of students about the potential exposure of their personal information. In all, about 20 UNLV students received the notice after a virus allowing remote access was discovered on a computer containing the students' personal information. According to Victor Barragan, CSUN Senate president and former sciences senator, there is no evidence that the information was leaked but the law requires the notification be sent. While an UNLV policy prohibits commenting on data breach specifics, the UNLV Information Security Office did urge students to monitor credit reports and financial statements if they were concerned over identity theft.

Links:

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

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

[3] <http://unlvrebelyell.com/2009/06/01/data-leak-raises-questions/>

VIRGINIA COMMONWEALTH UNIVERSITY NOTIFIES STUDENTS ABOUT POSSIBLE BREACH

Quick Facts

- Date: 6/5/09
- Institution: [Virginia Commonwealth University](#) [1]
- Type of Incident: Theft
- Number Affected: 17,214 (SSNs), 22,500 (Test Scores)
- Source: [OSF Data Loss DB](#) [2]
- Abstract Source: [The Washington Post](#) [3]

Abstract

Virginia Commonwealth University began notifying thousands of students after the theft of a computer containing sensitive information. The computer, stolen in mid-April from the VCU library, contained the names and Social Security numbers of 17,214 students and the names, VCU ID numbers and test scores of an additional 22,500 students. VCU police believe the thief quickly got rid of the computer and the chance the information was accessed is small. However, VCU officials will begin notifying credit agencies and government offices concerning the theft. VCU is offering one year of free credit monitoring services to the 17,214 students whose Social Security numbers were on the stolen computer.

Links:

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

[2] <http://datalossdb.org/incidents/2088-names-and-social-security-numbers-of-17-214-on-stolen-computer>

[3] <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/05/AR2009060501809.html>

EMAIL ATTACHMENT CONTAINS THE SOCIAL SECURITY NUMBERS OF 350 OSU STUDENT WORKERS

Quick Facts

- Date: 6/8/2009
- Institution: [Ohio State University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 350
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [The Lantern](#) [3]

Abstract

Ohio State University's Dining Services is working to protect student workers after an attachment containing sensitive information was accidentally sent in an email. The attachment contained the Social Security numbers of all 350 student workers and was accidentally attached to an email reminding student workers to sign waivers for the retirement program. According to OSU officials, the mistake was caught quickly and the IT department was able to stop many, but not all, emails before they were delivered to the recipient. OSU is offering affected students 12 months of credit protection through Debix at a cost to the university of \$11 per student that enrolls.

Links:

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

[2] <http://www.databreaches.net/?p=4676>

[3]

<http://media.www.thelantern.com/media/storage/paper333/news/2009/06/08/Campus/Dining.Services.Faces.Security.Debacle-3746546.shtml>

OREGON HEALTH & SCIENCE UNIVERSITY NOTIFIES PATIENTS AFTER LAPTOP THEFT

Quick Facts

- Date: 6/12/09
- Institution: [Oregon Health & Science University](#) [1]
- Type of Incident: Theft
- Number Affected: 1,000
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [KPTV](#) [3]

Abstract

Oregon Health & Science University (OHSU) is working to contact patients after a laptop containing patient information was stolen. The laptop, stolen from a physician's car, contained the names, treatment dates, treatment summaries and medical record numbers on about 1,000 patients. According to OHSU officials the laptop was password protected to avoid misuse of the data.

Links:

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

[2] <http://www.databreaches.net/?p=5555>

[3] <http://www.kptv.com/technology/19739721/detail.html>

KIRKWOOD COMMUNITY COLLEGE WARNS OF POTENTIAL DATA BREACH

Quick Facts

- Date: 6/12/2009
- Institution: [Kirkwood Community College](http://www.kirkwood.edu) [1]
- Type of Incident: Theft
- Number Affected: 1,600
- Source: [DataBreaches.net](http://www.databreaches.net) [2]
- Abstract Source: [TMCNet](http://www.tmcnet.com) [3]

Abstract

Kirkwood Community College (KCC) is working to notify individuals and businesses after the theft of a mobile storage device. The device, stolen on June 4th from the college's Skills to Employment office, contained the names and Social Security numbers of individuals and business contact information of participant program employers of the federally funded PROMISE JOBS program. The device was returned shortly after KCC staff notified authorities of the theft. However, computer experts examining the device were not able to assure the data had not been accessed.

Links:

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

[2] <http://www.databreaches.net/?p=5553>

[3] <http://www.tmcnet.com/usubmit/2009/06/12/4223796.htm>

LAPTOP CONTAINING UNIVERSITY OF NORTH DAKOTA DONOR INFORMATION STOLEN FROM CONTRACTOR

Quick Facts

- Date: 6/17/09
- Institution: [University of North Dakota](#) [1]
- Type of Incident: Theft
- Number Affected: 84,000
- Source: [ESI](#) [2]
- Abstract Source: [Post and Courier](#) [3]

Abstract

A laptop containing University of North Dakota donor information was recently stolen from the car of a contractor. The laptop, belonging to an employee of Blackbaud, Inc., contained information on 84,000 individuals. Blackbaud was hired to develop software for the university's foundation and alumni association. According to Blackbaud officials, the information on the laptop was encrypted and the theft was reported to the two university groups immediately. The company is working with the university groups to notify the affected individuals and help them monitor their credit reports. Blackbaud is also looking into why the employee had the information on the laptop top for a longer time period than they should have.

Updated 6/18 - Corrected typo in the title. Thanks to Allison Dolan for letting us know. - Adam

Links:

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

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

[3] http://www.postandcourier.com/news/2009/jun/17/stolen_laptop_contained_donors_financial86188/

JOHNS HOPKINS UNIVERSITY'S APPLIED PHYSICS LABORATORY'S WEB SITE BREACHED

Quick Facts

- Date: 6/17/09
- Institution: [Johns Hopkins University - Applied Physics Laboratory](#) [1]
- Type of Incident: Penetration
- Number Affected: *N/A*
- Source: [ESI](#) [2]
- Abstract Source: [The Baltimore Sun](#) [3]

Abstract

The Web site for the Johns Hopkins University's Applied Physics Laboratory (APL) has been taken off line as staff investigates a cyber attack discovered Sunday. The APL, which performs research on military and NASA projects, found that an unknown individual penetrated the Web site and gained access to unclassified information. According to APL officials, the attacker(s) did not gain access to any internal systems or classified information. While the investigation is still ongoing, it appears that the attack may have started two weeks ago. An APL spokesperson said that while the web site has had minor security breaches in the past, this recent attack has been one of the most significant to date.

Links:

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

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

[3] <http://www.baltimoresun.com/news/maryland/bal-md.hacking17jun17,0,3658700.story>

STOLEN CORNELL LAPTOP CONTAINS SENSITIVE INFORMATION ON STUDENTS, FACULTY AND STAFF

Quick Facts

- Date: 6/23/2009
- Institution: [Cornell University](#) [1]
- Type of Incident: Theft
- Number Affected: 45, 277
- Source: [ESI](#) [2]
- Abstract Source: [WVBR](#) [3]

Abstract

Cornell University is working to notify current and former students and staff after the theft of a laptop containing personal information. The laptop, which was being used to help diagnose transmission problems with the university's central administrative systems and does not appear that have been encrypted, contained the names and Social Security numbers of 22,546 current and former students and 22,731 current and former faculty and staff members. The laptop was stolen earlier this month but university officials did not learn of the theft until late last week. Cornell officials have sent an [email notification](#) [4] to all affected individuals and will be sending out letters shortly. Cornell has setup a [FAQ](#) [5] to help answer questions people may have about this theft.

Special thanks to David DyTang for making us aware of this incident. - Adam

Links:

- [1] <http://www.cornell.edu>
- [2] <http://www.adamdodge.com/esi>
- [3] <http://wvbr.com/news/660>
- [4] <http://wvbr.com/news/662>
- [5] <http://faq-june2009.cuinfo.cornell.edu/>

OREGON UNIVERSITY SYSTEM'S WEB SITE REPLACED WITH ANGRY MESSAGE ABOUT IRAN

Quick Facts

- Date: 6/24/2009
- Institution: [Oregon University System](#) [1]
- Type of Incident: Penetration
- Number Affected: *None*
- Source: [ESI](#) [2]
- Abstract Source: [The Wired Campus](#) [3]

Abstract

Recent visitors to the Oregon University System's main web site were greeted with an angry message to President Obama. It appears that a hacker was able to redirect traffic to the main web site to a site that claimed to be "from Iran". The redirect was up for about 90 minutes before staff became aware of the problem. While staff does not know exactly how the site was breached, officials say that staff will pay closer attention to the third party applications used to maintain the web site that do not automatically install updates.

Links:

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

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

[3] <http://chronicle.com/blogPost/Hackers-Rebuke-Obama-Via/7236>

STOLEN UCM REPORTS CONTAIN INFORMATION ON 7,000 STUDENTS

Quick Facts

- Date: 6/26/2009
- Institution: [University of Central Missouri](#) [1]
- Type of Incident: Theft
- Number Affected: 7,000
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [KMBC](#) [3]

Abstract

The University of Central Missouri is working to notify students after two reports containing personal information were stolen. The reports contained the names, dates of birth and Social Security numbers of 7,000 students enrolled between Summer 2005 and Summer 2006. UCMO has setup a web site - www.ucmo.edu/identityprotection [4] - with information to help students protect themselves and their identities.

Links:

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

[2] <http://www.databreaches.net/?p=5735>

[3] <http://www.kmbc.com/news/19873666/detail.html>

[4] <http://www.ucmo.edu/identityprotection/>

UCSD FLOODED WITH PHONE CALLS FOLLOWING COMPUTER

Quick Facts

- Date: 7/17/2009
- Institution: [University of California, San Diego](#) [1]
- Type of Incident: Penetration
- Number Affected: 30,000
- Source: [Personal Health Information Privacy](#) [2]
- Abstract Source: [Sign On San Diego](#) [3]

Abstract

Hundreds of concerned patients have been flooding the phone lines after the University of California San Diego's Moores Cancer Center suffered a computer breach. An unknown individual breached the Cancer Center's computers and stolen files on 30,000 patients containing names, dates of birth, medical record numbers, diagnoses and treatment dates back to 2004. The main concern among callers was the safety of their Social Security numbers. According to UCSD Health Sciences chief of marketing and communications officer DeAnn Marshall only 36 of the stolen files contained Social Security numbers. Following the breach, staff are working to review all security measures and taken any corrective measures if necessary.

Links:

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

[2] <http://www.phiprivacy.net/?p=1115>

[3] <http://www3.signonsandiego.com/stories/2009/jul/17/1m17hacker221630-hotline-ucsd-patients-swamped/>

FORMER PROFESSOR SUSPECTED IN KU LAPTOP THEFT

Quick Facts

- Date: 7/23/2009
- Institution: [Kansas University](#) [1]
- Type of Incident: Theft
- Number Affected: *Unknown*
- Source: [ESI](#) [2]
- Abstract Source: [KTKA](#) [3]

Abstract

Police investigating the theft of two laptop computers from Kansas University's Pharmacology and Toxicology department have found a suspect in a former KU professor. According to a police report, the professor in question failed to return the computers upon their resignation in March. The identity of the professor is being withheld and no arrests have been made at this point.

Links:

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

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

[3] http://www.ktka.com/news/2009/jul/23/former_ku_professor_suspected_theft_laptop_compu te/

STOLEN UCCS LAPTOP CONTAINED STUDENT INFORMATION

Quick Facts

- Date: 7/28/2009
- Institution: University of Colorado at Colorado Springs
- Type of Incident: Theft
- Number Affected: 766
- Source: [DataBreaches.net](#) [1]
- Abstract Source: [KRDO](#) [2]

Abstract

The University of Colorado at Colorado Springs has notified students after a laptop containing student information was stolen from the home of a faculty member. The laptop contained the names and grades of 766 students enrolled between 2003 and 2009. According to the university, the information, kept as part of class rosters, also could have contained the Social Security numbers of up to 241 of these students. According to a [statement](#) [3] by UCCS Executive Director of Information Technology Jerry Wilson, UCCS regrets the loss of student information and will continue working with departments to encrypt all personally identifiable data.

Links:

- [1] <http://www.databreaches.net/?p=6443>
[2] <http://www.krdo.com/Global/story.asp?S=10803897>
[3] <http://www.uccs.edu/~webdept/CMS/getnewscontent.php?id=963>

UTB STAFF ABUSE ACCESS TO BLACKBOARD TO CHEAT

Quick Facts

- Date: 8/1/2009
- Institution: [University of Texas, Brownsville](#) [1]
- Type of Incident: Employee Fraud
- Number Affected: *N/A*
- Source: [ESI](#) [2]
- Abstract Source: [Brownsville Herald](#) [3]

Abstract

The University of Texas, Brownsville and Texas Southernmost College police recently concluded a two-month long investigation uncovering gross academic fraud by staff of the Office of Distance Education. Police discovered that students and staff working in the Office of Distance Education used their access to the Blackboard system to steal test answers. Six staff and 14 student workers stole test answers for themselves, for friends and even to sell to other students. The theft occurred by staff and student workers that were given administrative access to the Blackboard system. According to other staff, the University had been made aware of possible cheating, but was not sure how to contain the problem. While no criminal charges will be filed, staff involved no longer work for the Office of Distance Education and students involved received a number of different punishments ranging from failing a course to suspension.

Links:

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

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

[3] <http://www.brownsvilleherald.com/news/online-100590-utb-employees.html>

DEGREE AUDITING SYSTEM SECURITY LAPSE MAKES UNIVERSITY OF OREGON GPAS VISIBLE ONLINE

Quick Facts

- Date: 8/2/2009
- Institution: [University of Oregon](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 20
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [Oregon Daily Emerald](#) [3]

Abstract

The University of Oregon quickly fixed a security hole in the university's degree auditing system, DuckWeb. The hole, discovered by Daniel Bachhuber a University of Oregon student, allowed DuckWeb users to access other student educational records by slightly changing the printer friendly view URL. According to University of Oregon Registrar Sue Eveland, the security hole would only have allowed access to around 20 student records. The information contained in the DuckWeb records vulnerable did not contain any Social Security numbers. According to Eveland, the only person to exploit the security hole was Bachhuber and this was the first time the university was made aware of the problem.

Links:

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

[2] <http://www.databreaches.net/?p=6545>

[3] <http://www.dailyemerald.com/news/security-lapse-makes-gpas-visible-1.236115>

BERKELEY SCHOOL OF JOURNALISM WEB SITE BREACH EXPOSES STUDENT INFORMATION

Quick Facts

- Date: 8/11/2009
- Institution: [University of California, Berkeley](#) [1]
- Type of Incident: Penetration
- Number Affected: 493
- Source: [OSF Data Loss DB](#) [2]
- Abstract Source: [UC Berkeley News](#) [3]

Abstract

The University of California, Berkeley is notifying students after a web server containing student information was breached. The web server, part of the university's School of Journalism, contained the personal information, dates of birth and Social Security numbers of 493 students that applied for admission between September 2007 and May 2009. While there is no evidence that the attacker gained access to the student data, the university issued the warnings to be safe. Staff became aware of the incident after launching an investigation into the claims that someone had breached the site. Staff worked quickly to repair the security vulnerability and the web site was placed back online.

Links:

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

[2] <http://datalossdb.org/incidents/2279-hacked-web-server-contained-a-database-with-493-applicants-names-dates-of-birth-and-social-security-numbers>

[3] http://www.berkeley.edu/news/media/releases/2009/08/11_data.shtml

LSU WEB SITE EXPOSES STUDENT INFORMATION

Quick Facts

- Date: 8/13/2009
- Institution: [Louisiana State University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: *Unknown*
- Source: [OSF Data Loss DB](#) [2]
- Abstract Source: [The Daily Reveille](#) [3]

Abstract

Louisiana State University is working to notify students after personal student information was found on an LSU web site. The web site, belonging to the university's College of Arts and Sciences, contained information such as student name and Social Security number. It is not known how many students were affected by the incident. LSU is offering free credit monitoring for all affected students.

Links:

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

[2] <http://datalossdb.org/incidents/2282-unknown-number-of-students-names-social-security-numbers-posted-on-university-web-site>

[3] <http://www.lsureveille.com/students-social-security-numbers-put-on-internet-12-30-p-m-1.1815684>

STOLEN NKU LAPTOP CONTAINS CURRENT, FORMER STUDENT INFORMATION

Quick Facts

- Date: 8/15/2009
- Institution: [Northern Kentucky University](#) [1]
- Type of Incident: Theft
- Number Affected: 200
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [NKY.com](#) [3]

Abstract

Northern Kentucky University is notifying current and former students after a laptop was stolen from a secured location on campus. Using a recent backup, the university was able to discover the laptop contained the names and Social Security numbers of 200 students. The university is advising students to place fraud alerts on their credit reports. While the university does not think that the information was what the thief was after, it will help student that find themselves a victim of identity theft due to the theft.

Links:

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

[2] <http://www.databreaches.net/?p=6722>

[3] <http://nky.cincinnati.com/apps/pbcs.dll/article?AID=/AB/20090815/NEWS0103/908160359/>

MASSIVE COMPUTER THEFT RAISES IDENTITY THEFT CONCERNS AT CSULA

Quick Facts

- Date: 8/18/2009
- Institution: [California State University, Los Angeles](#) [1]
- Type of Incident: Theft
- Number Affected: 600
- Source: [OSF Data Loss DB](#) [2]
- Abstract Source: [ABC](#) [3]

Abstract

California State University, Los Angeles is investigating a rash of computer thefts that contained the names and Social Security numbers of students and staff. The two computers and 12 laptops were found to contain the names, addresses and Social Security number of more than 600 CSULA individuals. According to the university, the students affected no longer attend the university. CSULA has setup a hotline - (800) 883-4029 - to help answer any questions students and staff have about the thefts.

Links:

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

[2] <http://datalossdb.org/incidents/2292-stolen-computers-expose-more-than-600-faculty-and-students-names-addresses-and-social-security-numbers>

[3] http://abclocal.go.com/kabc/story?section=news/local/los_angeles&id=6971986&rss=rss-kabc-article-6971986

FILE SHARING PROGRAM ON BU ROTC COMPUTER EXPOSES PERSONAL INFORMATION

Quick Facts

- Date: 8/20/2009
- Institution: [Boston University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 6,675
- Source: [OSF Data Loss DB](#) [2]
- Abstract Source: [Boston University News Release \(Data Loss DB archive\)](#) [3]

Abstract

Boston University is notifying several thousand students after personal information was found online. The files, belonging to the university ROTC program, contained the names and Social Security numbers of 6,675 individuals. According to the university, 406 of the individuals were BU students and the rest most likely belong to individuals involved with ROTC programs around the country. The files were accidentally released to the public in September 2008 after a file sharing program was installed on the computer without the consent of the university. The university worked quickly to remove the computer from the network once notified of the program. Boston University is offering free credit monitoring to all affected individuals.

Links:

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

[2] <http://datalossdb.org/incidents/2293-social-security-numbers-and-some-birth-dates-of-6-675-exposed-through-file-transfer-program>

[3] <http://datalossdb.org/archives/2293/3151/index.txt>

UMASS COMPUTER BREACH EXPOSES 20 YEARS OF PERSONAL DATA

Quick Facts

- Date: 8/21/2009
- Institution: [University of Massachusetts Amherst](#) [1]
- Type of Incident: Penetration
- Number Affected: *Unknown*
- Source: [ESI](#) [2]
- Abstract Source: [Telegram.com](#) [3]

Abstract

The University of Massachusetts Amherst recently announced the breach of a computer containing 20 years' worth of student information. The breach, which occurred between September 15 and October 27 of last year, involved a single server containing the names, Social Security numbers and a limited amount of credit card information on students that attended UMass between 1982 and 2002. While the university is not releasing the exact number affected, the breach does affect a large number of former graduate and undergraduate students. According to the university, while UMass was aware of the incident last fall, notification was delayed to allow for a full investigation. The university has placed a notice on its web site - www.umass.edu/computerintrusion/legal.html [4] - with more information for those affected by the incident.

Links:

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

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

[3] <http://www.telegram.com/article/20090821/NEWS/908210393/1116>

[4] <http://www.umass.edu/computerintrusion/legal.html>

UMASS COMPUTER BREACH EXPOSES 20 YEARS OF PERSONAL DATA

Quick Facts

- Date: 8/21/2009
- Institution: [University of Massachusetts Amherst](#) [1]
- Type of Incident: Penetration
- Number Affected: *Unknown*
- Source: [ESI](#) [2]
- Abstract Source: [Telegram.com](#) [3]

Abstract

The University of Massachusetts Amherst recently announced the breach of a computer containing 20 years' worth of student information. The breach, which occurred between September 15 and October 27 of last year, involved a single server containing the names, Social Security numbers and a limited amount of credit card information on students that attended UMass between 1982 and 2002. While the university is not releasing the exact number affected, the breach does affect a large number of former graduate and undergraduate students. According to the university, while UMass was aware of the incident last fall, notification was delayed to allow for a full investigation. The university has placed a notice on its web site - www.umass.edu/computerintrusion/legal.html [4] - with more information for those affected by the incident.

Links:

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

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

[3] <http://www.telegram.com/article/20090821/NEWS/908210393/1116>

[4] <http://www.umass.edu/computerintrusion/legal.html>

UNIVERSITY OF VERMONT ANNOUNCES CREDIT CARD BREACH

Quick Facts

- Date: 9/2/2009
- Institution: [University of Vermont](#) [1]
- Type of Incident: *Unknown*
- Number Affected: *N/A*
- Source: [ESI](#) [2]
- Abstract Source: [Consumer Loan Wire](#) [3]

Abstract

The University of Vermont recently announced that a number of university credit cards have been compromised. According to the university, up to 242 university-funded credit cards have been used for fraudulent activities. The university was notified of the compromise by the issuing bank. At this point, the university is not certain how the credit cards became compromised.

Links:

[1] <http://www.uvm.com>

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

[3] <http://www.consumerloanwire.com/news/210275-university-announces-credit-card-breach>

SECURITY BREACH AT UNIVERSITY OF FLORIDA

Quick Facts

- Date: 9/14/2009
- Institution: [University of Florida](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 34
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [University of Florida News](#) [3]

Abstract

The University of Florida announced a recently discovered security breach of personal information. The breach involved a file containing the 34 names and 25 Social Security numbers of trainers working with the Florida Traffic and Bicycle Safety Education program in 2006. The file the unsecured file was removed as soon as it was discovered by university techs during a routine security check. While the file was last modified in 2006, the university believes that the risk to personal information is low. The university has setup a web site - [privacy.ufl.edu/](#) [4] - and hotline - 877-657-9133 - to help answer questions about the incident.

Links:

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

[2] <http://www.databreaches.net/?p=7133>

[3] <http://news.ufl.edu/2009/09/14/notice-of-privacy-breach/>

[4] <http://privacy.ufl.edu/>

Quick Facts

- Date: 9/24/2009
- Institution: [Eastern Kentucky University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 5,045
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [Kentucky.com](#) [3]

Abstract

Eastern Kentucky University recently notified faculty, staff and student workers after a file containing Social Security Numbers was found online. The file, accidentally placed online in September 2008, contained the names and Social Security Numbers of 5,045 individuals on the EKU payroll in 2007-2008. According to EKU President Doug Withlock, the file could only be found by accessing the exact file name or by those that conducted a precise Google search. EKU has setup a web site - www.ecert.eku.edu [4] - and a hotline - 859-622-7777 - to help answer questions about the incident.

Links:

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

[2] <http://www.databreaches.net/?p=7486>

[3] http://www.kentucky.com/latest_news/story/947409.html

[4] <http://www.ecert.eku.edu>

[UPDATE1]SERVER CONTAINING UNC-CHAPEL HILL STUDY BREACHED

Quick Facts

- Date: 9/24/2009
- Institution: [University of North Carolina - Chapel Hill](#) [1]
- Type of Incident: Penetration
- Number Affected: 160,000 [Updated]
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [News-Record.com](#) [3]
- Update1 Source: [NewsObserver.com](#) [4]

Abstract

The University of North Carolina at Chapel Hill is working to notify thousands of women after a breach of a server containing a medical study was discovered. The server, one of two involved in a 14-year project analyzing mammography results, contained data on 236,000 women including 163,000 Social Security numbers. The breach was detected in July and UNC-Chapel Hill officials hired an outside forensic firm to help investigate the breach. After two months, the University still does not know who is responsible for the breach or if the data on the server was downloaded. According to the chairman of the UNC-CH Department of Radiology Matthew Mauro, the breach may have been as much as two years old. The breach has caused the UNC-CH Medical School to reevaluate all computer security measures. The University held off notification letters until the investigation was completed and will soon begin notifying all those affected.

Update1

The recent security breach at UNC-CH was less severe than first thought. According to officials, the files accessed contained information on 160,000 women including 114,000 Social Security numbers. The University has setup a hotline - 877-434-3065 - to help answer questions about the breach and the investigation.

Links:

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

[2] <http://www.databreaches.net/?p=7511>

[3] http://www.news-record.com/content/2009/09/25/article/hacker_hits_unc_chapel_hill_study_data

[4] <http://blogs.newsobserver.com/campusnotes/unc-security-breach-less-severe-than-thought>

STOLEN WILLIAMS COLLEGE LAPTOP CONTAINED PERSONAL INFORMATION

Quick Facts

- Date: 10/3/2009
- Institution: [Williams College](#) [1]
- Type of Incident: Theft
- Number Affected: 750
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [New Hampshire Department of Justice Breach Notification \(pdf\)](#) [3]

Abstract

Williams College recently disclosed that a stolen laptop contained sensitive information. The laptop, which was stolen from a Williams College car while parked off campus, contained the names and Social Security numbers of 750 individuals. Williams College staff worked to identify address information for these individuals, which they believe reside in 39 states. In the notification, Williams College is offering these individuals one year of credit monitoring.

Links:

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

[2] <http://www.databreaches.net/?p=8107>

[3] http://doj.nh.gov/consumer/pdf/williams_college.pdf

Quick Facts

- Date: 10/4/2009
- Institution: [Suffolk Community College](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 300
- Source: [ESI](#) [2]
- Abstract Source: [Newsday.com](#) [3]

Abstract

Suffolk Community College is offering credit monitoring after an email attachment containing Social Security numbers was accidentally sent out. The email contained an attachment with the names and Social Security numbers of 300 students. The mistake was discovered a day later and officials took action. The email server was shut down and the message was removed from accounts. In a second letter to the affected students, the college included instructions on how to take advantage of the credit monitoring.

Links:

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

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

[3] <http://www.newsday.com/long-island/suffolk/e-mail-error-sends-out-students-social-security-numbers-1.1499898>

BREACH CAUSES SHUTDOWN OF TUFTS WEBCENTER

Quick Facts

- Date: 10/6/2009
- Institution: [Tufts University](#) [1]
- Type of Incident: Penetration
- Number Affected: None
- Source: [ESI](#) [2]
- Abstract Source: [Tufts Daily](#) [3]

Abstract

An external attack caused Tufts University to shut down their WebCenter service. The attack involved 100 Tufts University computers that were compromised and used to send out spam email messages. According to the University, Tufts staff worked to block attackers coming from three different countries. The attack was discovered on Sunday and continued through Monday as IT staff noticed spikes in traffic from the affected machines. The attack involved computers in the University's Schools of Arts and Sciences and Engineering, the Tisch Library, Undergraduate Education, Student Affairs and Student Services (USS). The attack such a disruption that USS staff were sent home early if they felt they were not able to work productively. University staff worked to reinstall operating systems, increase password complexity and tweaked network controls. The WebCenter service was brought back online yesterday around 9pm.

Links:

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

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

[3] <http://www.tuftsdaily.com/it-security-breach-causes-webcenter-shutdown-1.1940619>

EMAIL HOAX TRACED TO UNIVERSITY OF COLORADO DENVER

Quick Facts

- Date: 10/9/2009
- Institution: [University of Colorado, Denver](#) [1]
- Type of Incident: Impersonation
- Number Affected: N/A
- Source: [ESI](#) [2]
- Abstract Source: [ABC 7 Denver](#) [3]

Abstract

An email hoax claiming the Denver Columbus Day parade was canceled was traced to a University of Colorado, Denver computer. The email, which claimed to be from president of the Sons of Italy Columbus Day Parade Committee Richard SaBell, was traced to a public kiosk computer at the university that is open for public use. Denver police have seized the computer and are conducting an investigation into the hoax. The person responsible could face charges of fraud and identity theft. In addition, the university is very concerned over this incident and considers the hoax unauthorized use of a campus computer.

Links:

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

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

[3] <http://www.thedenverchannel.com/news/21254446/detail.html>

STUDENT AND STAFF INFORMATION STOLEN FROM ROANE STATE EMPLOYEE'S CAR

Quick Facts

- Date: 10/12/2009
- Institution: [Roane State Community College](#) [1]
- Type of Incident: Theft
- Number Affected: 10,941
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [Roane State News Release](#) [3]

Abstract

Roane State Community College is working to notify current and former students and employees after the theft of a device containing personal information. The device, stolen from the care of a Roane State employee, contained the names and Social Security Numbers of 1,194 current and former employees and 9,747 current and former students. Roane State staff also determined that the device contained only the Social Security Numbers for an additional 5,036 current and former students. The employee's car was broken into while off campus and the theft is being investigated by the Konx County Sheriff's Department. Roane State has sent letters to all affected individuals and is offering one year of credit monitoring. The device did not contain educational records.

Links:

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

[2] <http://www.databreaches.net/?p=7912>

[3] <http://www.roanestate.edu/keyword.asp?keyword=IDALERT>

MULTI-COMPUTER UNIVERSITY OF WISCONSIN-MADISON BREACH EXPOSES PERSONAL INFORMATION

Quick Facts

- Date: 10/12/2009
- Institution: [University of Wisconsin, Madison](#) [1]
- Type of Incident: Penetration
- Number Affected: 3,000
- Source: [ESI](#) [2]
- Abstract Source: [Fox 6 Now](#) [3]

Abstract

The University of Wisconsin, Madison recently notified faculty, staff and students after a breach may have exposed personal information. The breach, which involved multiple computers over several months, may have exposed up to 3,000 names and Social Security Numbers. In total, University officials believe that 40 computers were breached and used to distribute illegal copies of music, movies television shows and software. Wisconsin-Madison staff became aware of the breach on August 31 and investigation shows most of the illegal access occurred over the past 18 months. However, the earliest breach occurred in December 2001. In an October 12 letter to affected individuals, University officials say there is no evidence that personal information was accessed.

Links:

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

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

[3] <http://www.fox6now.com/news/sns-ap-wi--uw-computershacked,0,28958.story>

CSULA FACULTY MEMBER MISTAKENLY POSTS FILES WITH STUDENT DATA ONLINE

Quick Facts

- Date: 10/14/2009
- Institution: [California State University, Los Angeles](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 85
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [KTLA](#) [3]

Abstract

California State University, Los Angeles is working to notify students and faculty after personal information was mistakenly placed online. The information, placed on the Web by a CSULA faculty member, contained the names and Social Security numbers of 82 students and 3 faculty members. The exposure involves individuals enrolled in CIS 454 or 528 in Spring 2002 and CIS 283 and 585 in Spring 2003. The information was the faculty member's web site back in July. Once CSULA became aware of the problem, the files were immediately removed. CSULA is working to notify all affected individuals as well as working to make sure such a mistake does not happen in the future. CSULA College of Business and Economics has setup a toll-free hotline - 800-883-4029 - to help answer questions about the incident.

Links:

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

[2] <http://www.databreaches.net/?p=7817>

[3] <http://www.ktla.com/news/landing/ktla-csula-computer-breach,0,1880242.story>

STUDENT AND ALUMNI DATA ON STOLEN BLOOMSBURG UNIVERSITY

Quick Facts

- Date: 11/1/2009
- Institution: [Bloomsburg University of Pennsylvania](http://www.bloomu.edu) [1]
- Type of Incident: Theft
- Number Affected: 574
- Source: [OSF Data Loss DB](http://datalossdb.org) [2]
- Abstract Source: [Bloom U Today](http://www.bloomtoday.com) [3]

Abstract

Bloomsburg University of Pennsylvania recently announced that the theft of a university laptop may have exposed personal student information. The laptop, stolen from a university office, contained the names, Social Security numbers and grades of 574 current and former students. The theft appears to affect students enrolled in psychology courses taught by Julie Kontos from Summer 2004 to Spring 2006. The laptop was stolen along with several small devices and Bloomsburg University Police are investigating the theft. In the notification letter, Bloomsburg advises students to sign up for credit monitoring.

Links:

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

[2] <http://datalossdb.org/incidents/2419-stolen-laptop-may-contain-social-security-numbers-of-574>

[3]

<http://www.bloomtoday.com/default.asp?sourceid=&smenu=1&twindow=&mad=&sdetail=1053&wpage=1&skeword=&si date=&ccat=&ccatm=&restate=&restatus=&reoption=&retype=&repmin=&repmax=&rebed=&rebath=&subname=&pform=&sc=2533&hn=bloomtoday&he=.com>

MISTAKE EXPOSES PERSONAL INFORMATION OF CHAMINADE UNIVERSITY STUDENTS

Quick Facts

- Date: 11/6/2009
- Institution: [Chaminade University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 4,500
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [Star Bulletin](#) [3]

Abstract

Chaminade University recently announced that a mistake exposed personal information on thousands of students. According to the university a report that was mistakenly placed online contained the names and Social Security numbers of 4,500 students. The investigation determined that the report was placed online eight months ago and affected enrolled undergraduate students that attended the university between 1997 and 2006. Chaminade became aware of the mistake on Wednesday and immediately removed the report from the Internet. Chaminade University has created a web site - www.chaminade.edu/infosecure [4] - to help answer questions about the incident.

Links:

- [1] <http://www.chaminade.edu>
- [2] <http://www.databreaches.net/?p=8142>
- [3] <http://www.starbulletin.com/news/breaking/69438757.html>
- [4] <http://www.chaminade.edu/infosecure>

Quick Facts

- Date: 11/15/2009
- Institution: [California State Polytechnic University, Pomona](http://www.csupomona.edu) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 355
- Source: [ESI](http://www.adamdodge.com/esi) [2]
- Abstract Source: [LA Times](http://www.latimes.com/news/local/la-me-cal-poly16-2009nov16,0,503569.story) [3]

Abstract

California State Polytechnic University, Pomona recently announced that a mistake exposed the personal information of former applicants online. The information, available online for five years, included names and Social Security numbers of 355 applicants from 2003. According to the university, the information was mistakenly placed in a publicly accessible folder in November 2003. The file was removed in November 2008, but the data remained in search engine caches and indexes. Cal Poly Pomona became aware that this information was still, in part, available when a former student discovered his own information while searching Google.

Links:

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

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

[3] <http://www.latimes.com/news/local/la-me-cal-poly16-2009nov16,0,503569.story>

Quick Facts

- Date: 11/19/2009
- Institution: [University of East Anglia](http://www.uea.ac.uk) [1]
- Type of Incident: Penetration
- Number Affected: UNKNOWN
- Source: [ESI](http://www.adamdodge.com/esi) [2]
- Abstract Source: [Examiner.com](http://www.examiner.com) [3], [The Register](http://www.theregister.co.uk) [4]

Abstract

The University of East Anglia's Hadley Climate Research Center recently suffered a breach exposing thousands of email messages. The breach involved 1079 e-mail messages and 72 documents containing internal communications from researchers involved in global warming research. These documents were uploaded to an anonymous FTP server. The documents and e-mails themselves contain internal communications filled with crude language and disparaging comments on skeptical scientists. In addition, several of the messages appear to bring into question the relationship between the scientists and several journalists as well as call into question the methodologies used in some of the research.

Links:

[1] <http://www.uea.ac.uk>

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

[3] <http://www.examiner.com/x-28973-Essex-County-Conservative-Examiner~y2009m11d19-Hadley-CRU-hacked-with-release-of-hundreds-of-docs-and-emails>

[4] http://www.theregister.co.uk/2009/11/20/cru_climate_hack/

Quick Facts

- Date: 11/20/2009
- Institution: [Notre Dame](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 24,000
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [WNDU](#) [3]
- Update1 Source: [The Observer](#) [4]

Abstract

Notre Dame is warning employees after files containing personal information were discovered online. The files, accidentally placed online, contained names, Social Security numbers and dates of birth of an unreleased number of university employees. According to a spokesperson, the university removed the file as soon as the incident was discovered and there is no evidence the information was misused.

Update1

In total, the personal information on about 24,000 Notre Dame employees, including some student workers, was accidentally made available online.

Links:

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

[2] <http://www.databreaches.net/?p=8360>

[3] <http://www.wndu.com/localnews/headlines/70674717.html>

[4] <http://www.ndsmcobserver.com/news/24-000-employees-affected-by-data-breach-1.979963>

Quick Facts

- Date: 11/24/2009
- Institution: [University College Dublin](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: 2
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [The University Observer](#) [3]

Abstract

The University Observer, a student newspaper, was able to obtain detailed academic records on two University College Dublin students from UCD. The newspaper, with the knowledge and consent of the two students, filed official requests for information using nothing more than publicly available information. These requests were accepted and the newspaper was supplied with full academic statements on these students. In response to the ease with which the University Observer was able to obtain these records, UCD Students' Union President Gary Redmond asked the university to "...review its internal policies to ensure that all procedures were followed in this instance, and if necessary introduce mechanisms to ensure that a breach of this nature does not occur in the future." The university declined to comment on whether or not the university would be reviewing data protection procedures.

Links:

[1] <http://www.ucd.ie>

[2] <http://www.databreaches.net/?p=8414>

[3] <http://www.universityobserver.ie/2009/11/24/university-hands-confidential-student-records-to-media/>

NEBRASKA LINCOLN COMPUTER BREACH AFFECTS HIGH SCHOOL GRADUATES

Quick Facts

- Date: 12/4/2009
- Institution: [University of Nebraska Lincoln](#) [1]
- Type of Incident: Penetration
- Number Affected: 4,000
- Source: [DataLossDB.org](#) [2]
- Abstract Source: [The Doings Clarendon Hills](#) [3]

Abstract

The University of Nebraska Lincoln began notifying high school graduates after discovering a security breach involving a computer containing personal information. The server, used as part of a student the university was conducting on the practices of school districts and standardized test performances, contained the names, Social Security numbers and ACT test score information on 4,000 high school graduates between 2002 and 2005. The information was gathered from the ACT organization with the permission of the Hinsdale High School District 86, Glenbard District 87 and schools in South Sioux City. An investigation into the incident discovered the computer was not adequately secured which allowed unauthorized external access to the computer and the information. In the letters sent to the 4,000 individuals, the university is offering one year of LifeLock identity theft protection.

Links:

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

[2] <http://datalossdb.org/incidents/2436-hacked-computer-contains-names-addresses-and-social-security-numbers-of-4-000>

[3] <http://www.pioneerlocal.com/clarendonhills/news/1921349,hi-d86security-120409-s1.article>

EASTERN ILLINOIS UNIVERSITY ADMISSIONS SERVER COMPROMISED BY VIRUS

Quick Facts

- Date: 12/4/2009
- Institution: [Eastern Illinois University](#) [1]
- Type of Incident: Penetration
- Number Affected: 9,000
- Source: [ESI](#) [2]
- Abstract Source: [EIU Notice to Students](#) [3], [Daily Eastern News](#) [4]

Abstract

Eastern Illinois University recently began notifying current and former students as well as applicants after discovering a security breach involving a server containing applicant information. The server, used by the Office of Admissions, contained the electronic applications for admissions between March 10, 2000 and November 16, 2009. These applications contained names, Social Security numbers, dates of birth, mailing addresses and other contact information on 9000 individuals. The university discovered the server was participating in a botnet on November 16 and took action to remove the server from use. An investigation discovered the server was compromised on November 11. While university officials state there is no evidence anyone accessed the applicant data, Eastern is offering those affected a one year membership for identity theft protection through Experian. When asked about the three week delay in notifying affected individuals, Adam Dodge, Eastern's IT Security Officer, stated that many factors contributed to delay including an in-depth investigation by Dodge's office, gathering information on the individuals on the server, collecting and verifying address information, and contracting with Experian.

Links:

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

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

[3] <http://www.eiu.edu/notice/>

[4]

<http://media.www.dennews.com/media/storage/paper309/news/2009/12/07/News/Viruses.Infect.Admissions.Server-3846441.shtml>

VALDOSTA INVESTIGATES SERVER BREACH

Quick Facts

- Date: 12/11/2009
- Institution: [Valdosta State University](#) [1]
- Type of Incident: Penetration
- Number Affected: *Unknown*
- Source: [ESI](#) [2]
- Abstract Source: [Valdosta State University News Release](#) [3]

Abstract

Valdosta State University is working to notify current and former faculty and students after staff discovered unauthorized access on a server. The server contained the names, Social Security numbers and grades of students from 1997 to present and faculty from 1996 to present. The unauthorized access was discovered on December 11, 2009 and appears to date back to November 11, 2009. VSU's University Police and Division of Information Technology are investigating the breach along with help from Georgia's Bureau of Investigations. At this point, the university has not determined if personal data was accessed or transferred.

Links:

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

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

[3] <http://www.valdosta.edu/news/releases/computer.121109>

DAYTONA STATE COLLEGE EMAIL SYSTEM HACKED, USED TO SEND BOMB THREATS

Quick Facts

- Date: 12/11/2009
- Institution: [Daytona State College](#) [1]
- Type of Incident: Penetration, Impersonation
- Number Affected: 1
- Source: [ESI](#) [2]
- Abstract Source: [Daytona Beach News-Journal \(via Google Cache\)](#) [3]

Abstract

Daytona Beach Police are investigating the breach of Daytona State College's email system after the system was used to send out three bomb threats. The bomb threat emails were sent from the hacked system to one of the college's adjunct professors. The emails, which originated from an account belonging to an employee on the Daytona Beach campus, contained references to bombs and a threat to "blow this school up, and kill everyone till they are gone". According to John Banker, the college's security supervisor, the employee was not responsible and someone had hacked into her account. Daytona State College does not feel this is a viable but is taking steps to locate the person responsible.

Links:

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

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

[3] <http://74.125.95.132/search?hl=en&source=hp&q=cache:http://www.news-journalonline.com/NewsJournalOnline/News/WestVolusia/wvWEST02121109.htm&aq=f&oq=&aqi=g10>

UCSF DOCTOR FALLS VICTIM TO PHISHING SCAM

Quick Facts

- Date: 12/15/2009
- Institution: [University of California, San Francisco](#) [1]
- Type of Incident: Penetration
- Number Affected: 600
- Source: [PHIPrivacy.net](#) [2]
- Abstract Source: [San Francisco Business Times](#) [3]

Abstract

The University of California, San Francisco has alerted patients after a physician's email account was compromised. The email account contained demographic and clinical information as well as some Social Security numbers on 600 patients. The email account became compromised in mid-October after the physician fell victim to a phishing scam. According to UCSF news director Corinna Kaarlela, these 600 individuals were notified starting October 21 and December 11, 2009 which is the period during which the university conducted an in-depth investigation into the incident. While the investigation uncovered no indication the emails were accessed, individuals potentially affected were urged to carefully review statements from health insurers for suspicious payments and immediately report any discrepancies to their insurance provider.

Links:

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

[2] <http://www.phiprivacy.net/?p=1638>

[3] <http://www.bizjournals.com/sanfrancisco/stories/2009/12/14/daily32.html>

NORTH CAROLINA COLLEGES LIBRARY SYSTEM BREACHED

Quick Facts

- Date: 12/17/2009
- Institution: [Alamance Community College](#) [1], [Beaufort County Community College](#) [2], [Bladen Community College](#) [3], [Blue Ridge Community College](#) [4], [Brunswick Community College](#) [5], [Central Carolina Community College](#) [6], [College of The Albemarle](#) [7], [Gaston College](#) [8], [Halifax Community College](#) [9], [Haywood Community College](#) [10], [Johnston Community College](#) [11], [Lenoir Community College](#) [12], [Martin Community College](#) [13], [Nash Community College](#) [14], [Pamlico Community College](#) [15], [Piedmont Community College](#) [16], [Richmond Community College](#) [17], [Roanoke-Chowan Community College](#) [18], [Rowan-Cabarrus Community College](#) [19], [Sandhills Community College](#) [20], [Southwestern Community College](#) [21], [Tri-County Community College](#) [22], [Vance-Granville Community College](#) [23], [Wake Tech Community College](#) [24], [Wilson Community College](#) [25]
- Type of Incident: Penetration
- Number Affected: 51,000
- Source: [DataBreaches.Net](#) [26]
- Abstract Source: [NC Community Colleges Press Release](#) [27] (PDF)

Abstract

The North Carolina Community Colleges system began notifying library patrons from 25 NC community colleges after an unauthorized individual gained access to a system housing patron data. The affected server, located in the NC Community Colleges System Office, was found to contain the personal information on 51,000 individuals including 12,400 Drivers License number and 38,500 Social Security numbers. The breach appears to have occurred on August 23, 2009 and NC Community Colleges staff became aware of the breach on August 24, 2009. An initial review discovered that 18 colleges used the Driver's License information to identify patrons. These colleges include Alamance, Beaufort, Blue Ridge, Brunswick, Central Carolina, College of The Albemarle, Gaston, Halifax, Johnston, Martin, Pamlico, Piedmont, Richmond, Rowan-Cabarrus, Tri-County, Vance-Granville, Wake Tech and Wilson. On October 19, 2009, the ongoing investigation uncovered that 12 colleges used Social Security numbers to identify patrons. these colleges include Bladen, Haywood, Lenoir, Nash, Pamlico, Richmond, Roanoke-Chowan, Sandhills, Southwestern, Tri-County, Vance-Granville and Wilson. The letters sent to those affected inform the individuals whether their Driver's License number or Social Security number (or both) were on the server and the letters contain information on how to check and secure credit profiles. NC Community Colleges are working to ensure that all personal data is removed from library systems to help prevent this incident from occurring in the future. The press release did not give a reason for the long delay in notification.

Links:

- [1] <http://www.alamancecc.edu>
- [2] <http://www.beaufortccc.edu>
- [3] <http://www.bladencce.edu>
- [4] <http://www.brcc.edu>
- [5] <http://www.brunswickccc.edu>
- [6] <http://www.cccc.edu>
- [7] <http://www.albermarle.edu>
- [8] <http://www.gaston.edu>
- [9] <http://www.halifaxcc.edu>
- [10] <http://www.haywood.edu>
- [11] <http://www.adamdodge.com/esi/www.johnstoncc.edu>

- [12] <http://www.lenoircc.edu>
- [13] <http://www.martincc.edu>
- [14] <http://www.nashcc.edu>
- [15] <http://www.pamlicoacc.edu>
- [16] <http://www.piedmontcc.edu>
- [17] <http://www.richmondcc.edu>
- [18] <http://www.roanokechowan.edu>
- [19] <http://www.rowancabarrus.edu>
- [20] <http://www.sandhills.edu>
- [21] <http://www.southwesterncc.edu>
- [22] <http://www.tricountycc.edu>
- [23] <http://www.vgcc.edu>
- [24] <http://www.waketech.edu>
- [25] <http://www.wilsoncc.edu>
- [26] <http://www.databreaches.net/?p=8926>
- [27] [http://www.ncccs.cc.nc.us/news_releases/Library Server Press Release 121709.pdf](http://www.ncccs.cc.nc.us/news_releases/Library_Server_Press_Release_121709.pdf)

[UPDATE1]MALWARE POTENTIALLY EXPOSES PENN STATE STUDENT INFORMATION

Quick Facts

- Date: 12/18/2009
- Institution: [Penn State University](#) [1]
- Type of Incident: Penetration
- Number Affected: 30,000 (Updated)
- Source: [Data Loss DB](#) [2]
- Abstract Source: [Penn State Live](#) [3]
- Update1 Source: [Pittsburgh Post-Gazette](#) [4], [DataBreachs.net](#) [5]

Abstract

Penn State University is alerting former students after a computer containing personal information was compromised by malware. The computer, found to be infected with malware and communicating to computers outside of the university, contained an archived class list with 261 Social Security numbers. The university removed the infected computer from the network as soon the problem was discovered. According to PSU's chief privacy officer, Sarah Morrow, there is no reason to believe the student information was accessed but Penn State decided to err on the side of caution. As Morrow stated, "Even when theft is only a remote possibility, we alert anyone who may have been affected, and arm them with information and steps to take to mitigate their risk."

Update1

Pennsylvania State University has begun notifying individuals after a large scale malware outbreak was discovered. The outbreak, affecting multiple computers, involved systems containing the names and Social Security numbers of around 30,000 individuals. The systems affected belonged to the Eberly College of Science (7,758 records), the College of Health and Human Development (6,827 records) and Penn State Schuylkill (15,000 records). According to Penn State spokeswoman Annemarie Mountz the Social Security numbers were contained in archived files on the systems affected by the malware and the university does not have any indication the files were accessed. Instead the letters, containing information on protecting against identity theft, were sent out as a precaution. As a result of this and a previous breach this year at Penn State's Behrend campus, Penn State has started initiatives to safeguard information stored on university-owned computers.

Links:

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

[2] <http://datalossdb.org/incidents/2482-infected-computer-potentially-exposes-hundreds-of-social-security-numbers>

[3] <http://live.psu.edu/story/43583>

[4] <http://www.post-gazette.com/pg/09364/1024438-298.stm>

[5] <http://www.databreaches.net/?p=9325>

WESTERN MICHIGAN UNIVERSITY WEB SITE ACCIDENTALLY EXPOSES STUDENT INFORMATION

Quick Facts

- Date: 12/22/2009
- Institution: [Western Michigan University](#) [1]
- Type of Incident: Unauthorized Disclosure
- Number Affected: *Unknown*
- Source: [DataBreaches.net](#) [2]
- Abstract Source: [New Hampshire Attorney General's Office](#) [3] (PDF)

Abstract

Western Michigan University has notified students after a mistake exposes student information online. According to the letter to the NH Attorney General's Office, student information, such as Social Security numbers, was inadvertently exposed online for "a brief period of time". The information was discovered on December 14, 2009 and the information was immediately removed. According to the university, there is no evidence the information was accessed, letters were sent out offering those affected a one-year membership in a credit monitoring service by IDExperts.

Links:

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

[2] <http://www.databreaches.net/?p=9449>

[3] http://doj.nh.gov/consumer/pdf/western_michigan_university.pdf

EASTERN WASHINGTON UNIVERSITY BREACH AFFECTS 130,000

Quick Facts

- Date: 12/31/2009
- Institution: [Eastern Washington University](#) [1]
- Type of Incident: Penetration
- Number Affected: 130,000
- Source: Data Loss [2]
- Abstract Source: [Seattle PI](#) [3]

Abstract

Eastern Washington University will soon be notifying current and former students following a severe breach. The system contained the names, dates of birth and Social Security numbers of 130,000 students dating back to 1987. The breach was discovered during a security assessment in early December. The investigation into the incident discovered that the system was breached and used to store video files. While the university does not have any evidence the information was accessed inappropriately, letters are being sent out as a precaution. In the letter to affected individuals, EWU President Rodolfo Arevalo stated that the university is treating the breach seriously and will continue to upgrade systems and security practices to protect sensitive information. EWU has setup a web site - www.ewu.edu/x67128.xml [4] - with more information on the breach.

Links:

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

[2] <http://datalossdb.org/incidents/2493-unknown-security-breach-exposes-130-000-students-names-and-social-security-numbers>

[3] http://www.seattlepi.com/local/413738_eastern31.html

[4] <http://www.ewu.edu/x67128.xml>