Out of the Boardroom, into the Classroom: Information Security in Higher Education

Eric J. Rzeszut, CISSP, University of Alabama at Birmingham (UAB)

ABSTRACT: Just like Fortune 500 corporations, academic institutions need to protect their data. Yet the expectations, budgets, procedures, and levels of cooperation in these organizations can differ significantly from those in the corporate world. Common security tools and training are often aimed at formal business environments, and may not be applicable to other groups. Academic institutions also have specific legislation, such as FERPA, which have serious ramifications for data security. From several case studies and the presenter's own experience, learn the pitfalls and peculiarities involved in bringing acceptable levels of security to these institutions; and the unique requirements and challenges of working with faculty and students.

Just like in the corporate world, data at academic institutions can be compromised:


The Wenatchee WORLD

HOME | NEWS | SPORTS | OPINION | OBITUARIES | A&E | LIFESTYLE | BLOG

9 free views left!

WVC accidentally releases Social Security numbers

College advises former students to place fraud alerts on credit files

By Rachel Schlerf
World staff writer

Thursday, March 31, 2011

WENATCHEE — Wenatchee Valley College accidentally released Social Security numbers of students who attended classes there 10 years ago.

The college sent letters of apology to more than 3,800 former students Monday, and urged them to place fraud alerts on their credit files as a precautionary step.

The mistake happened as the college responded to a public records request from a local law firm asking for 10 years of financial records.

Until fall 2002, the college's record system tracked students by their Social Security numbers instead of student identification numbers.

In December, the college sent 84,000 pages of data in the response to the request and inadvertently included the Social Security numbers. A student analyzing the data found the numbers and alerted the college on March 24, said Fiscal Services Director Jonah Nicholas.

Nicholas said it's hard to say how many of those 3,800 former students were included in the records release, but he sent letters to students who attended WVC before 2002, just in case.


UNIVERSITY OF HAWAI'I - WEST O'AHU

About UHWO | Admissions | Programs & Services | Academics | Offices & Services | Campus Life

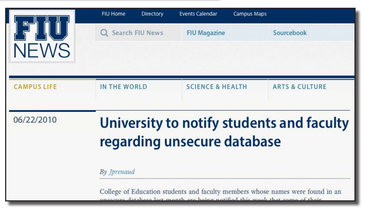
UNIVERSITY of HAWAI'I WEST O'AHU News Release

NEWS RELEASE
October 29, 2010

UH WEST O'AHU ANNOUNCES INADVERTENT EXPOSURE OF SENSITIVE STUDENT INFORMATION

PEARL CITY – The University of Hawai'i – West O'ahu (UHWO) is notifying approximately 40,000 individuals that their personal information may have been compromised.

The exposure occurred when a faculty member inadvertently uploaded files containing data including names, social security numbers, addresses, birth dates and educational information to an unsecured database. The files contained information on students who attended the University of Hawai'i at Manoa from 1990 – 1998 and during 2001. In addition, students who attended UHWO during Fall of 1994 or graduated from 1988 - 1993 may also be affected.


FIU NEWS

FIU Home | Directory | Events Calendar | Campus Maps

Search FIU News | FIU Magazine | Sourcebook

CAMPUS LIFE | IN THE WORLD | SCIENCE & HEALTH | ARTS & CULTURE

06/22/2010

University to notify students and faculty regarding unsecure database

By Jeremiah

College of Education students and faculty members whose names were found in an

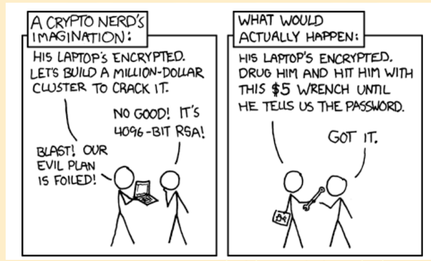
What are the unique challenges to information security in higher education?

- **Decentralization:** historically, universities have had very decentralized IT operations; this leads to non-standard, non-documented setups.
- **Autonomy:** especially at research universities like UAB, faculty control their own budgets, personnel, equipment, etc.
- **Diverse computing environment:** unlike corporate world, not standardized platforms. High numbers of Macs at most universities; Linux boxes; proprietary research software/hardware.
- **Transient population:** students graduate/transfer, new freshman/ transfers enter, faculty move to/from other institutions.
- **Relaxed environment:** generally, items like dress codes, work hours, etc. are less structured in academic when compared to the corporate world. These attitudes can spill over into information security.

Case Study: Encryption at UAB

Background:

- In March 2009, UAB's president signed a mandate requiring all laptop hard drives to be encrypted.
- This applied (and continues to apply) to all laptops used for "UAB business," regardless of ownership.
- Departments with their own IT staff were responsible for their unit's laptops; laptops in units without their own IT personnel are encrypted by central IT.



used with permission, xkcd.com

Reactions/responses from faculty:

"Most of us (labrat-types) do not keep confidential information on our laptops and it is a difficult sell to convince us that unencrypted data on our last chromatography experiment is going to compromise anyone's privacy."

"If a laptop gets stolen with microscope images of cells on it who cares?"

"Please take it [encryption software] off. It takes forever to boot up when I try and give talks."

"What even qualifies as 'UAB data?' The only data even related to UAB on my laptop is my research. There's nothing pertaining to HR, patient care, or anything else I can imagine the university caring much about."

Reactions/responses from IT personnel:

"Unless there is patient data on a machine, there is no reason for mandatory encryption; I can guarantee that it will only be an invitation for more problems for IT at UAB."

"While your concept sounds great in theory, try applying it to folks who generate the money that pays you who do not want this technology on their machines."

"For machines that have no sensitive information encryption is a waste of time. What's going to happen is we are going to tighten this campus down so much it becomes impossible or very burdensome to get anything done."

Lessons Learned:

*3.5 years after the mandate, central IT estimates that **no more than 60%** of covered laptops are encrypted.*

Why? Several possible explanations:

1. ***Enforcement.*** *The encryption mandate is only enforced **retroactively**, if a faculty or staff member loses a laptop. There is no campuswide proactive checking/reporting. Individual unit chairmen/ directors often don't take the time to enforce.*
2. ***Communication.*** *The mandate, and its repercussions, have never been clearly disseminated to the wider campus community.*
3. ***Autonomy.*** *For reasons discussed at at right, research faculty control their own "kingdoms," and don't necessarily recognize the authority of central IT over "their" computers.*
4. ***Mistrust.*** *Due to the historic decentralization at UAB, the central IT department is a relatively new unit, without a great reputation. Faculty simply don't trust them.*

Universities have two constituent groups not found in the corporate world; groups that don't have clear analogs outside academia

FACULTY

- Faculty (especially research faculty) have a great deal of autonomy.
- UAB CDIB has 45 faculty members -- in many ways, this means that the administrative staff have 45 distinct supervisors!
- The faculty in our department secure most of their own "extramural" funding (via grants from NIH, NSF, American Cancer Society, etc.) and make most of their own fiscal decisions.
- **Money is power:** Our faculty members manage over $12.5 million in outside research funding (as of 6/2012).
- Academia is highly competitive. Universities regularly "poach" well-funded faculty from other institutions.
- Faculty, in effect, grow accustomed to "being their own bosses": They hire/fire employees, accept students into their labs, purchase equipment as budget allows, and run their own kingdoms.

"Many academic institutions, just like hospitals, put these employees [faculty] on a pedestal and cater to their wants. They are often allowed to dictate what security measures they will and won't tolerate rather than allowing knowledgeable security and systems administrators to make the decisions on security controls."

Ronald Woerner, **CISSP,** Professor & Director, CyberSecurity Studies
College of Information Technology, Bellevue University

STUDENTS

- Students are not employees, so employee-focused discipline or training doesn't work.
- Students expect to be able to use their wireless devices anywhere on campus, at any time, for any purpose -- content filtering/restriction not found on most campuses.
- Universities have to decide – does student/faculty/staff traffic all use the same wireless network, same authentication scheme? Or are students placed in a "walled garden," a separately-managed network? What about the additional costs and workload of that configuration?

Contact Information:
Eric J. Rzeszut, CISSP
Information Systems Specialist III
Department of Cell, Developmental and Integrative Biology
University of Alabama at Birmingham
ericrz@uab.edu : **@ericrz**
http://cdib.uab.edu : **@CDIBatUAB**