

Security breaches challenge academia's 'open society'

Jay Cline

June 7, 2005 ([Computerworld](#))

While all the attention lately has been focused on security breaches at our nation's data consolidators, U.S. universities have also been notifying thousands of employees, students and alumni to monitor their personal accounts for unusual activity. The University of Iowa recently became at least the 16th college this year to publicly disclose a breach of its information security (see table).

What's going on? Have hackers opened up a campaign against our colleges?

The answer is probably no. Computer-savvy students have been probing and exploiting university networks for a long time, ever since the 1983 movie *War Games* glorified the teenage hacker.

It's likely that we're hearing about these university breaches now because of the California Security Breach Notification Act, which went into effect in January. The act requires notification of California residents if unauthorized users may have accessed their sensitive information. The law has effectively resulted in the notification of all potentially affected people, however, because no organization wants to be seen as caring about the safety of only Californians.

But I don't think we're going to see a drop-off in the number of university breach notices anytime soon. Why? Because a number of factors have converged to put colleges uniquely at risk to ongoing compromises of their information security.

The most fundamental factor is the openness of the university. The free and open exchange of ideas has long been at the core of the university mission. As a result, the typical campus is physically open to all comers; no identification badge is needed. Its intellectual property is openly aired, and

members of the college community interact in public forums online and off-line. Names of professors are public knowledge much more often than their middle-management counterparts in private industry, and rosters of students aren't hard to come by, either. The campus is like this because everyone there, except IT security, wants it that way.

But what's the risk of this openness? When it comes to IT security, it means there's more opportunity for social engineering—for a hacker to impersonate a targeted individual in obtaining his access credentials.

A more recent phenomenon contributing to college IT risk has been the widespread webification of university business processes. Within less than a generation, the typical campus environment has transformed itself from bricks-and-ivy to clicks-and-ivy. The list of processes that have made their online debut is a long one:

- New-student application and selection
- Course registration, instruction and testing
- Grade distribution
- Instructor evaluation
- Financial-aid application and awarding
- Dorm-room selection
- Library accounts
- Campus purchases
- Tuition billing and payment
- Campus and alumni directories

How does this colossal move online affect IT security? By bringing more offline information into the realm of what the hacker can access remotely. Universities that still use the Social Security number as a student ID are even more vulnerable, because that single piece of information can often be used as the key to unlock many of these online accounts.

A third trend challenging campus IT departments is the dynamic nature of their student users. The annual turnover of IT users at a four-year college can top 15%, a rate not seen by most companies. And each year, the incoming freshman class demands an IT environment that accommodates the latest technical innovations, such as camera phones, BlackBerry devices and wireless laptops.

The result is a college IT department that has fewer options than its industry counterparts to enforce security standards for devices, applications and network access.

All of these vulnerabilities add up. As of March, universities had accounted for 28% of the 50 security breaches recorded by the state of California since 2003, more than any other group. Financial institutions followed with 26%.

This isn't to fault the campus IT departments for not doing their level best. Some of the best thinking on enterprise security architectures—a comprehensive approach to the design of security technologies and processes within an organization—has come from academia, and universities were among the first to implement such architectures. I think many of us in industry would be impressed with what they've been able to do within their resource and policy limitations.

But if publicized security breaches in academia continue at the current pace, colleges will be pressured to rethink their approach and commitment to the openness of their learning environments. Members of academic communities won't tolerate having their identities at risk.

What are colleges doing about it? I've noticed a few common themes among those hit by security breaches:

1. Replacing the Social Security number with a university ID number and personal identification number as the primary authenticators for campus transactions
2. Providing regular training and awareness to the university community on good security practices for their personal devices and information
3. Advertising a central phone number and e-mail address for the university community to report suspected security breaches

Based on the nature of the reported breaches, universities should also consider allocating more resources to patching known vulnerabilities in their systems. They should also at least evaluate the "nuclear option" of implementing stored-data encryption.

Ultimately, university administrations may be forced into a debate about who belongs—and who doesn't belong—in their college communities. Campus IT leaders should avoid taking sides in that debate, but should stand at the ready to finally implement the security measures they've been recommending for years.

Academe Exposed

Security breaches have hit at least 16 U.S. universities so far this year, potentially exposing the information of more than a half-million people.

Month incident publicized (2005)	University	Number of people potentially affected	Type of security breach
June	University of Iowa	30,000	intentional unauthorized access
May	Stanford University	9,600	intentional unauthorized access
May	Purdue University	11,360	intentional unauthorized access
May	Middle Tennessee	unspecified	intentional unauthorized

	State University		access
April	Florida International University	unspecified	unintentional exposure
April	Michigan State University	40,000	intentional unauthorized access
April	Tufts University	106,000	unusual activity identified
April	Carnegie Mellon University	19,000	unintentional exposure
April	Georgia Southern University	unspecified	intentional unauthorized access
March	University of California, Berkeley	98,369	intentional theft of laptop
March	Boston College	120,000	intentional unauthorized access
March	California State University, Chico	59,000	intentional unauthorized access
March	Northwestern University	21,000	intentional unauthorized

			access
January	University of California, San Diego	3,500	intentional unauthorized access
January	Kansas University	unspecified	intentional unauthorized access
January	George Mason University	32,000	intentional unauthorized access
TOTAL		549,829+	