Hacking Higher Ed

The cybersecurity challenge on college campuses lies as much with the students as with malicious outsiders.

By David F. Carr

PLUS When education gets too virtual
COVER STORY
4 Hacking Higher Ed
Outsiders aren’t the only threat to cybersecurity on campus. Don’t forget the threat from within.

3 Commentary
Students can use technology to undermine the integrity of education.

11 Editorial and Business Contacts

MORE INFORMATIONWEEK EDUCATION
Check Out Our Education Website
InformationWeek Education brings the enterprise IT credentials and credibility of InformationWeek, providing news, analysis and expert commentary on the technology issues reshaping higher ed.
informationweek.com/education

IN-DEPTH REPORTS
Pay Lags For Education IT
Salaries for IT pros in higher education have been flat, but workers get satisfaction from job perks such as flexibility
informationweek.com/reports/2013edsalary

Apple Outlook
Some of our survey respondents in education are re-evaluating their commitment to Apple’s products.
informationweek.com/reports/appleoutlook

PREVIOUS ISSUE
Analytics Put To The Test
Can data analysis keep students on track and boost college retention rates? Also in this issue: Higher ed is just as prone to tech-based disruption as other industries.
informationweek.com/ed/feb2013
The visions of how technology can help students learn are promising. The reality of how students can use technology to undermine the integrity of education is already here.

This issue’s cover story begins with a recent news item about two students at Ohio’s Miami University who used keylogger devices to capture professor passwords and gain access to an online grade book. They were arrested and expelled after admitting to changing grades for themselves and others.

In a similar case at California’s Palos Verdes High School in January 2012, three students were charged with first breaking into the janitor’s office to steal a classroom master key. They reportedly planted keylogging devices on multiple computers, mined passwords, and used them to alter scores on tests and homework just enough to bump grades up a bracket. The three students set up a commercial operation, charging $300 to boost a grade from a B to an A, according to the Los Angeles Times. They were charged with burglary and conspiracy to commit burglary.

My 12-year-old son has been known to do a little shoulder surfing to capture the “learning coach” password his mom and I use on the online educational website K12.com. He and his sister are in a virtual school, so getting the password let him grade some of his own schoolwork. The good news is that he isn’t as clever as he thinks he is and routinely gets stopped when he tries a tactic like this one. My hope is that as he matures, he’ll learn the lesson that it’s more rewarding to actually do the work.

The Palos Verdes High School students were apparently smart kids, taking honors and AP classes. It’s unclear whether they needed to inflate their own grades. None of the news stories I’ve read reports how they were caught, but it seems likely that news of their “enterprise” got back to school officials. At Miami University, a professor noticed that the grades in the online system didn’t match her paper notes. To make such exploits easier to detect, the university’s technology team is modifying its grade book software to send an email notification to instructors whenever grades are changed so they can confirm the legitimacy of those changes.

Academic cheating is nothing new. Like many of the ills associated with unauthorized use of computer systems, digitization just provides new techniques and temptations.

Do online education tools make cheating easier? Maybe, but in all of the examples cited above, cheating was thwarted by people who care about education and were paying attention. Should my son’s grades get an inexplicable boost, or his latest essay show better spelling, grammar and vocabulary than he has produced before, his mom will know and have a talk with him. The Miami University students apparently tried to cover their tracks by changing grades for other students in addition to themselves. However, once investigators started looking at the pattern of grade changes across multiple courses, it wasn’t hard to see a couple of students turning up as the common denominator.

As the digitization of education continues, “auditing a course” may take on a whole new meaning, as educators seek better ways to verify that grades reflect actual learning.

David F. Carr is editor of InformationWeek Education. Read more by him at informationweek.com/davidfcarr. Write to him at david.carr@ubm.com.
The cybersecurity challenge on college campuses lies as much with the students as with malicious outsiders.

When a faculty member at Miami University in Oxford, Ohio, logged into the university’s grade book last fall, she realized something was wrong: The grades in the online system didn’t match her paper records. She was alert enough to see this was no mere glitch.

In March, after months of investigation, police charged two students with hacking the system to inflate grades. Police maintain that Beckley Parker, 21, of Weston, Conn., had changed his own grades for 17 classes since the spring of 2011, and also changed grades...
for 50 other students, according to the Dayton Daily News. David Callahan, 22, of Cambridge, Mass., reportedly changed his own grade once and two other students’ grades. Although the facts are subject to interpretation, it seems the two were either trying to help fraternity brothers or other friends at the same time they were improving their own grades, or they may have been trying to cover their tracks by changing more than one grade in each case.

All it took for them to make the changes was an inexpensive keylogger device, inserted between the keyboard and the computer it was attached to, which allowed them to record the actions of teachers entering their passwords for the grading system. They were then able to access the system at will.

After cooperating with investigators, the students avoided being charged with a felony, instead accepting dismissal from the university and pleading guilty to multiple counts of “attempted unauthorized use of property,” a misdemeanor.

Miami University’s information security officer, Joe Bazeley, says an attack on the university’s learning and grading systems is actually worse than the sort of attacks, namely information theft and exposure, that used to keep him up at night before the keylogger incident. “We produce knowledge and identify that via grades and a diploma,” Bazeley says. The grade book hack “challenges the integrity of those grades and diplomas,” he says.

Learn From The Hacks

Unfortunately, examples abound in higher education of the other kind of security breach. An undergraduate at the University of Nebraska last year was able to break into a database associated with the university’s PeopleSoft system, exposing Social Security numbers and other sensitive information on about 654,000 students, alumni and employees. According to our sister website Dark Reading, the university was lucky enough to detect the breach and shut it down quickly. An IT staffer picked up on an error message that seemed like evidence of something amiss, and a recently installed security information and event management system helped network managers sort through system logs and collect enough evidence to allow police to get a warrant to confiscate the computer of the student believed to have been behind the attack.

In March, Salem State University in Massachusetts alerted 25,000 current and former students and staff that their Social Security numbers may have been compromised in a database breach. If the pattern of the last few years repeats itself, expect higher education institutions to experience another half dozen major security breaches by the end of 2013.

As these examples show, information security risks to colleges and universities include...
threats to both privacy and academic integrity, and they’re as likely to come from inside as outside the campus. Even in the absence of malicious intent, students have been known to wander into some of the sketchier neighborhoods on the Internet in search of free music and movie downloads, which may come with a bonus helping of malware. Therefore, every laptop or student device that connects to the campus network must be treated with a degree of suspicion.

Servers and PCs in computer labs have been known to turn up as nodes in botnets used to attack other targets. Some of those threats originate with foreign powers, but that fact shouldn’t necessarily conjure up visions of hacks on universities being executed from some war room in China, says Doug DePeppe, an attorney and consultant who teaches in the University of Maryland University College cybersecurity master’s program. “If the objective is just to turn up as nodes in botnets used to attack other targets, why go through the difficulty?” DePeppe says. “Which makes it a little easier to say, ‘We’re in the same boat as everyone else, and of course we’ll respond.’ Of course, you’d still hate to have to make that case if an incident occurs.”

Rather than worrying about their reputations, colleges and universities should be worrying about the legal liability they could incur if they fail to take reasonable precautions. “It’s the modern-day slip-and-fall case, now on the Internet,” DePeppe says.

Protecting college information systems is uniquely challenging because security measures tend to run contrary to student and faculty expectations of openness and unfettered access and must be introduced with a light touch. “If you’re working in the banking sector, you’re going to have a preference for security, but in academia the whole idea is to share information and expand horizons,” DePeppe says. “In order to do that, there has to be openness.”

No Security Anywhere

Today, the risk that security breaches pose to a university’s reputation is probably lessened by the sheer number of examples in the news, DePeppe says. “There’s a growing recognition that nobody is secure,” he says, “which makes it a little easier to say, ‘We’re in the same boat as everyone else, and of course we’ll respond.’ Of course, you’d still hate to have to make that case if an incident occurs.”

No Security Anywhere

Today, the risk that security breaches pose to a university’s reputation is probably lessened by the sheer number of examples in the news, DePeppe says. “There’s a growing recognition that nobody is secure,” he says, “which makes it a little easier to say, ‘We’re in the same boat as everyone else, and of course we’ll respond.’ Of course, you’d still hate to have to make that case if an incident occurs.”

Rather than worrying about their reputations, colleges and universities should be worrying about the legal liability they could incur if they fail to take reasonable precautions. “It’s the modern-day slip-and-fall case, now on the Internet,” DePeppe says.

Despite their tradition of openness, educational institutions must inventory their digital systems and assess the risks they face. For example, tools such as learning management systems pose less of a risk for theft of private information than back-end administrative systems, but an LMS could pose a risk for grade manipulation, DePeppe says.

Case Western Reserve University’s chief information security officer, Thomas Siu, says the worst thing he has heard of students doing with an LMS is hop onto a computer used for entering grades can use a keylogger to capture the instructor’s password. These devices are inserted between the keyboard plug and the computer. KeeLog.com has a basic model that records data internally for about $50. The $150 KeyGrabber Wi-Fi Premium model (shown here) will periodically email you its logs, making it unnecessary to return to the scene of the crime.
class is canceled. Nevertheless, he sees risks everywhere. “If someone asks me, ‘Is this secure?’ I never say yes or no. I say, ‘What is our risk?’” Siu says.

Case Western operates a relatively flat network, rather than segmenting it into student, faculty and administrative networks, he says. The risk tolerance in a university environment is higher than in the corporate world, out of necessity, Siu says. “Our job is to be open, have high access and let you experiment,” he says.

The risks escalate when university systems are “balkanized” — when departments and other fiefdoms outside of the IT organization make their own technology choices, Siu says. Harvard and other universities are known for operating like a consortium of schools or departments that manage their own technology, with the richest ones having more to invest in security and everything else, he says. “Case is more centralized than most,” Siu says, “but we’re still about 50-50.”

To succeed as an information security pro in that environment, “don’t think you can control people,” he says. “Instead, you have to cajole them into using your resources.” When it comes to approving new systems or applications, information security leaders must position themselves as helping “enable the revolution in education,” rather than getting in the way, he says. “You need a willingness to wave the flag and say, ‘Hey, guys, you didn’t think this through.’ But you need to be able to do it with a smile and a joke.”

David A. Curry, director of information security at
New York’s The New School, says the threats he faces now are less intense than the ones he faced in prior positions in the financial services industry. But in some ways that makes it more challenging to remain vigilant. “It’s harder to make the argument that stuff needs to be protected,” Curry says. “You can’t just say: Because the regulation says so. When I used to work in financial services, it was always very easy to implement things that way.”

Still, The New School does have a regulatory responsibility to protect student data, as well as a commercial interest in protecting its reputation, he adds.

What Curry worries about more is doing a better job of training faculty and staff on information security risks and the proper handling of sensitive data. “The potential for mistakes is there,” he says, “and that probably worries me more than any particular hacker attack type of thing.”

Recognize The Threats

Others working in higher education see a “more corporate” approach to information security taking hold. “Before, a school would never have a CISO, a chief information security officer,” says Pete Trimarchi, technical director at New York Law School. “Now you’re starting to see that,” especially as colleges and universities collect more personally identifiable information and are legally responsible for protecting it. (Perhaps that’s a particular danger if you’re in the business of educating future lawyers.)

As threats multiply, Trimarchi plans to install a more sophisticated Layer 7 firewall, one that can “block at the application level, rather than the port level,” he says.

Meanwhile, the law school has implemented ForeScout CounterACT for network access control, particularly for use with student access over the wireless network. One of the key considerations for this choice was that the product is Web-based, requiring only a browser plug-in to scan student laptops and certify them as malware-free before letting them onto the network. The law school’s previous access control system required installing an application on each user’s computer and wound up generating far too many help desk calls when students couldn’t get it to work properly. Users also reported that the software interfered with their access from home. The new software has allowed Trimarchi to free up two people who previously spent most of their time handling help desk calls for more productive work, he says.

Protecting data from outside threats is important, Trimarchi says, but he has come to realize that insider threats — when student devices get hijacked by an attacker — are more significant. “We don’t have a lot of stu-
dents who come in trying to hack our systems," he says.

Research shows that the younger the college student, the more likely he is (and it’s most often a he) to try to fix his grades or engage in other unethical computer activity. A soon-to-be-published paper co-written by Yair Levy, who runs the Center for e-Learning Security Research at Nova Southeastern University, concludes that 92% to 95% of students surveyed about their attitude toward manipulating electronic learning systems are “purely ethical,” Levy says. However, “there’s a smaller group, which we found out is particularly young males, 18 to 20, who think doing that is completely acceptable — not only that, it’s cool,” he says.

Levy worries that students with strong hacking skills could decide to cripple e-learning servers to buy time to complete assignments. “So then they can say, ‘Oops, there is a technical problem. Let’s get an extension,’ ” he says. “We’ve seen those things happening.”

In the survey of 519 business students from a state university and a community college, the younger students were a little more likely than older students to rate as acceptable activities including attacks on a server, unauthorized access and intercepting someone else’s email. This finding is consistent with other research that shows ethical judgment improving with age, possibly related to developmental stages in the brain, Levy says. Age also builds resistance to peer pressure, he says.

**How To Spot Illicit Hardware**

The keylogging approach used at Miami University is particularly difficult to guard against, since it requires no advanced skills, just access to an inexpensive keylogger device. You can buy them on the Web for $50 or less, or spend about $150 for a premium Wi-Fi version that lets you capture data from a distance. Using such devices isn’t illegal in all cases; employers, for example, can use them to monitor the activity of suspect employees, and parents can use them to spy on the computer use of their children.

Bazeley has found no reliable way of detecting the devices with an automated scan, so the best defense is visual. Miami University is deploying all-in-one workstations that should help by making the keyboard connection to the device more visible. On older computers, a simple fix is to plug the keyboard into one of the USB ports on the front of the machine, rather than the back, so that the presence of a foreign object inserted in that slot isn’t likely to be missed.

In addition, Miami University is modifying the software for its Sakai and Banner grade
book systems so that educators will get an alert whenever a grade change is recorded. Think of this modification as the equivalent of the notifications you get from Web services asking if you just changed your password, though Bazeley says there will be a detailed log of all changes.

Even if universities have become more businesslike, their IT operations are still very different from their corporate equivalents, he says. When Bazeley worked in the corporate world, he says, “we had much stronger powers. If I said, ‘This machine is bad, take it off the network,’ that happened immediately.” At a university, it’s a longer process of consulting with the faculty member responsible for the suspect computer to make sure academic freedom won’t be infringed by shutting the machine down. The university environment also provides more opportunities for attackers because of the diversity of operating systems and configurations on computers around campus, only some of which conform to IT department recommendations.

“On the positive side, I’m seeing more awareness,” Bazeley says. “I have a lot of faculty members who are interested in the security of their grade book all of a sudden, who weren’t a year ago.” Part of his job, he says, is to “capitalize on the incident” to get everyone at the university to be more careful.

Write to David F. Carr at david.carr@ubm.com. Read more by him at informationweek.com/davidfcarr.
Business Contacts

Chief Sales Officer, Media, Martha Schwartz
(212) 600-3015, martha.schwartz@ubm.com

Sales Specialist, Sal Silletti
(212) 600-3029, salvatore.silletti@ubm.com

SALES CONTACTS—WEST
Western U.S. (Pacific and Mountain states) and Western Canada (British Columbia, Alberta)
Western Regional Sales Director, Sandra Kupiec
(415) 947-6922, sandra.kupiec@ubm.com

Strategic Account Director, Coretta Wright
(415) 947-6245, coretta.wright@ubm.com

District Sales Manager, Vanessa Tormey
(805) 252-4357, vanessa.tormey@ubm.com

Account Manager, Ashley Cohen
(415) 947-6349, ashley.i.cohen@ubm.com

Strategic Accounts
Account Director, Vesna Beso
(415) 947-6104, vesna.beso@ubm.com

SALES CONTACTS—EAST
Midwest, South, Northeast U.S. and Eastern Canada (Saskatchewan, Ontario, Quebec, New Brunswick)
District Manager, Jenny Hanna
(516) 562-5116, jenny.hanna@ubm.com

District Manager, Michael Greenhut
(516) 562-5044, michael.greenhut@ubm.com

District Manager, Cori Gordon
(516) 562-5181, cori.gordon@ubm.com

Inside Sales Manager East, Ray Capitelli
(212) 600-3045, raymond.capitelli@ubm.com

Strategic Accounts
District Manager, Mary Hyland
(516) 562-5120, mary.hyland@ubm.com

Account Manager, Tara Bradeen
(212) 600-3387, tara.bradeen@ubm.com

SALES CONTACTS—MARKETING AS A SERVICE
Director of Client Marketing Strategy, Jonathan Vlock
(212) 600-3019, jonathan.vlock@ubm.com

Director of Client Marketing Strategy, Julie Supinski
(415) 947-6887, julie.supinski@ubm.com

SALES CONTACTS—EVENTS
Senior Director, InformationWeek Events, Robyn Duda
(212) 600-3046, robyn.duda@ubm.com

MARKETING
VP, Marketing, Winnie Ng-Schuchman
(631) 406-6507, winnie.ng@ubm.com

Sr. Marketing Manager, Monique Luttrell
(949) 223-3609, monique.luttrell@ubm.com

Promotions Manager, Angela Lee-Moll
(516) 562-5803, angela.lee-moll@ubm.com

UBM TECH
Paul Miller
CEO
Robert Faletta
CEO, Channel
Marco Pardi
President, Events
Sandra Wallach
CFO
David Michael
cio
Martha Schwartz
Chief Sales Officer, Media
Simon Carless
Exec. VP, Game & App Development and Black Hat
Lenny Heymann
Exec. VP, New Markets
Angela Scalpello
Sr. VP, People & Culture

Rob Preston
VP and Editor In Chief
rob.preston@ubm.com
516-562-5692

Lorna Garey
Content Director, Reports
lorna.garey@ubm.com
978-694-1681

Sek Leung
Associate Art Director
sek.leung@ubm.com

David F. Carr
Editor
david.carr@ubm.com
954-757-5827

Chris Murphy
Editor
chris.murphy@ubm.com
414-906-5331

Jim Donahue
Chief Copy Editor
james.donahue@ubm.com

Stacey Peterson
Executive Editor, Quality
stacey.peterson@ubm.com
516-562-5933

Mary Ellen Forte
Senior Art Director
maryellen.forte@ubm.com

READER SERVICES
InformationWeek.com
The destination for breaking IT news, and instant analysis

Electronic Newsletters
Subscribe to InformationWeek Daily and other newsletters at informationweek.com/newsletters/subscribe.html

Events
Get the latest on our live events and Net events at informationweek.com/events

Reports
reports.informationweek.com
for original research and strategic advice

How to Contact Us
informationweek.com/contactus.html

Editorial Calendar
informationweek.com/edcal

Back Issues
E-mail: customerservice@informationweek.com
Phone: 888-664-3332 (U.S.)
847-763-9588 (Outside U.S.)

Reprints
Wright’s Media, 1-877-652-5295
Web: wrightsmedia.com/reprints/?magid=2196
E-mail: ubmreprints@wrightsmedia.com

List Rentals
Specialists Marketing Services Inc.
E-mail: PeterCan@SMS-Inc.com
Phone: (631) 787-3008 x3020

Media Kits and Advertising Contacts
createyourenextcustomer.com/contact-us

Letters to the Editor
E-mail: iwletters@ubm.com
Include name, title, company, city and daytime phone number.

Subscriptions
Web: informationweek.com/magazine
E-mail: customerservice@informationweek.com
Phone: 888-664-3332 (U.S.)
847-763-9588 (Outside U.S.)

Copyright 2013 UBM LLC. All rights reserved.