Hacking incidents prompt universities to rethink balance of openness, security

March 21 2014

In the two weeks between recent revelations that hackers stole data on students, alumni and faculty from the University of Maryland-College Park and the Johns Hopkins University, nearly 360,000 records were swiped in similar attacks at schools in Pennsylvania, Indiana and North Dakota.

Online thieves have increasingly sought sensitive or otherwise valuable data from educational institutions, experts say. Last year alone, breaches included possible exposure of 2.5 million Social Security and bank account numbers associated with an Arizona community college system, 74,000 Social Security numbers of University of Delaware students and staff, and 145,000 applications to Virginia Tech, according to the Privacy Rights Clearinghouse.

Colleges and universities often are attractive targets for hackers because there are many access points into their networks, which contain not just financial and personal data but also valuable intellectual property. That threat is forcing academics to reassess the way they keep and protect vast collections of information, often held in decentralized computer networks accessible to thousands of students, professors and researchers.

"It's been a long-standing concern that our culture of collaboration and trust kind of flies in the face of the need for security to be more closed, more alert and more skeptical and cynical," said Rodney Petersen, senior policy adviser for SecuriCORE, a higher-education information security project at Indiana University. Just as campuses have added gates, guards

and surveillance cameras on in recent decades, they may have to end the era of open access to online resources, he said.

The University of Maryland and other institutions reeling from major data thefts are redoubling efforts to confine and protect sensitive data spread across networks - sometimes so scattered that it's a complicated task simply to learn where the data might be hiding and vulnerable. The growing security risks may also require new barriers around networks that have been traditionally open in the name of academic discourse and unfettered access.

But unlike retailers, banks and other companies that guard sensitive data, universities can't mandate what devices or software are used to access their networks. And they must accommodate students and researchers spread across the globe, making it more difficult to prevent and detect security breaches.

Since January 2013, more than 50 colleges, universities and school systems across the country have been the targets of attacks that may have compromised personal information, according to the Privacy Rights Clearinghouse, a California-based consumer-advocacy group.

Such attacks are not confined to colleges and universities. The school systems in Maryland's Howard and Carroll counties, for example, have reported network disruptions linked to possible cyberattacks this year, though personal data was not thought to have been at risk in either case.

Since a breach compromised names, Social Security numbers and birth dates of 287,580 students, faculty and staff at the University of Maryland on Feb. 18, officials said they have purged more than three-fourths of the sensitive records, some of which dated back to 1992. But they are also hastening to learn how vulnerable the university's data remains, and how to prevent future attacks.

A cybersecurity task force that university President Wallace Loh called together within 24 hours of the attack is set to consider whether information technology systems on campus should be centralized to keep sensitive data in one place, rather than scattered across various colleges and departments. The group, which met for the first time last week, also is launching an effort to scan all university databases for personal information that could be at risk.

Similar actions have taken place at Johns Hopkins, where officials on March 6 announced an attack that occurred late last year compromising names and email addresses of 848 biomedical engineering students, as well as confidential evaluations of classmates. In response to attacks and at the urging of auditors, the university has moved to prioritize what data needs the highest levels of protection, said Darren Lacey, the university's chief information security officer.

Cybersecurity experts familiar with educational institutions' challenges fending off hackers said the strategies are common responses to the growing threats. While they have traditionally used "open coffee-house style" networks, institutions are increasingly rearranging how they organize business systems such as tuition processing or employee payroll, said James Robinson, director of security for Accuvant, a cybersecurity company that works with higher-education clients.

That sort of strategy is one of their few options, given the broad access allowed on a university network. While a company can control what technology their employees use to connect remotely - often through secure virtual private networks - universities don't have that luxury. And though security measures typically include automated systems that look for unusual activity or known malicious actors, that can be like finding a needle in a haystack.

Lacey said of Hopkins' monitoring efforts, "Really, everything is an

anomaly. If I get a million connections from another country, a corporation might say, 'That's not good.' In our world, because we have students and faculty all over the world, that doesn't necessarily trigger any response from us."

Meanwhile, officials are increasingly sifting through a deluge of questionable activity.

"Here at UMB, the number of attempts to get unauthorized access to our networks has grown exponentially over the last five or six years, where our intrusion-prevention system blocks literally millions of attempts every day," said Peter J. Murray, chief information officer at the University of Maryland-Baltimore.

He said 90 percent or more of the millions of emails sent to the university each week originate from websites "blacklisted" by anti-spam software providers. Those emails, which are blocked, often try to fool people into providing information such as passwords, credit card details or money. Many hacking efforts come through programs freely available on the Internet.

The simple response has been to do a better job of isolating sensitive personal data and building up protections around it, though that can invite more pursuit by hackers seeking to profit from theft. There may be other cases in which hackers are after valuable research data or other intellectual property, but they likely aren't publicized because there is no legal mandate to report them, Robinson said.

As logical as it sounds, though, it's not an easy transition for large institutions. On a campus like the one in College Park, IT systems and other back-office functions are spread across multiple colleges, each with multiple departments within it.

"It's a cultural shift" to take some of those responsibilities away and shift them to a central university authority, Peterson said.

Hopkins officials said they are transitioning to a more corporate-like network, consolidating business systems with sensitive data and placing controls on how that data is used, pushing people to "be somewhat more circumspect in what data they need," Lacey said.

At UM-College Park, the university's cyber task force has not yet determined how security practices vary across the campus and which present vulnerabilities, Ann Wylie said. The university last scanned its databases for personal information in 2006, so it's also unclear if there are places sensitive information is harbored unprotected, she said.

Some experts suggest that access to some parts of university networks should nonetheless be limited, cutting down on the points through which hackers could gain access. One option: so-called two-step verification, forcing users who log in on a new device with a username and password to then provide a code sent via text message or email, Robinson said.

But higher-education officials may be reluctant to compromise the openness of their networks, at the risk of disrupting research that involves sharing large amounts of data, whether or not that data is sensitive. Tighter security could particularly challenge computer science research seeking to learn more about the very attacks officials hope to avoid.

"I think things are going to get a lot harder for everyone," said Matthew Green, an assistant research professor of computer science at Johns Hopkins. "It's good to be secure, but it's good to be open. You have to really be careful how much you do to prevent people from the work they're supposed to be doing."

Officials say they are striving for a balance. At the UM-College Park, Wylie said sensitive student data might be sequestered without affecting research activity, though the university's task force could determine that research data on human subjects, survey responses or valuable intellectual property could afford stricter controls.

"There is a tension here, but I think we can work with that tension," she said. "We do not want to do anything that would put barriers for our faculty and grad students and researchers to do their work."

—-

EXAMPLES OF BREACHES:

-Sept. 28, 2013: Virginia Tech reveals 144,963 online applications to the university may have been accessed. No Social Security numbers or financial data were exposed but nearly 17,000 driver's license numbers were.

-Nov. 27, 2013: Names, Social Security numbers, bank account information and dates of birth for 2.5 million people associated with the Maricopa County Community College district in Phoenix, Ariz., may have been exposed.

-Dec. 13, 2013: Names, Social Security numbers and tax identification numbers of 6,500 individuals associated with the University of North Carolina-Chapel Hill were mistakenly posted online.

-Feb. 19, 2014: The University of Maryland-College Park says the Social Security numbers and birth dates for 309,079 students, alumni, faculty and staff were exposed in a breach. It later revises the number downward to 287,580 when some incomplete or inaccurate data is discovered in the database.

-Feb. 26, 2014: Indiana University announces personal data, including Social Security numbers, of 146,000 students and alumni were breached.

-March 6, 2014: North Dakota University System notifies students, staff and faculty that 290,780 personal records, including Social Security numbers, were exposed in a breach.

-March 6, 2014: The Johns Hopkins University says the names and contact information of 1,307 students and faculty were exposed when a hacker attempted to extort the university for further access to its servers. It later lowered the number to 848.