THE CHRONICLE

of Higher Education®

chronicle.com

March 21, 2014
Volume LX, Number 27

Data Breaches Put a Dent in Colleges' Finances as Well as Reputations

By MEGAN O'NEIL

INDIANA U.

At Indiana U.'s data center, in Bloomington, staff members were aghast to learn that the university was among several in recent weeks to come upon security breaches in their information-tecŸology operations.

The costs of a cyberattack on the University of Maryland that was made public last month will run into the millions of dollars, according to data-security professionals who work in higher education. Such a financial and reputational wallop threatens many colleges that are vulnerable to serious data breaches, experts say.

Crystal Brown, chief communications officer at Maryland, says an investigation into the theft of 309,079 student and personnel records, dating to 1998, is being led by the U.S. Secret Service. As part of its response, the university has contracted with outside forensics experts and is notifying all affected individuals. It is also providing five years' worth of free credit-protection services to all those affected.

A tally of costs related to the breach is not yet available, Ms. Brown says. But several data-security professionals interviewed by *The Chronicle* say the total will reach seven figures.

"You are talking about 300,000 people spread across the continental U.S. and you offered them all credit monitoring, and you had a lawyer, and you had an IT forensics firm—my very conservative estimate would be a couple million dollars," says Paul G. Nikhinson, a manager of privacy-breach-response services with the Beazley Group, which sells cybersecurity insurance to colleges.

The Maryland case is one of several data-security breaches reported by colleges in recent weeks. On February 25, Indiana University said a staff error had left information on 146,000 students exposed for 11 months. A week later, the North Dakota University system reported that a server containing the information of 291,465 former, current, and aspiring students and 784 employees had been hacked.

Few institutions budget in advance for data breaches, according to college officials and data-security professionals. Cybersecurity insurance in higher education remains a rarity, despite a consensus among those working in the field that the likelihood of such a breach involves "when," not "if."

The list of potential expenses is long. It includes forensics consultants, lawyers, call centers, websites, mailings, identity-protection and credit-check services, and litigation. Breaches can prompt major campus projects, such as risk-management reviews, campuswide encryption, and tests to determine how vulnerable networks are.

"For the organization itself, it is like a multiheaded hydra," Mr. Nikhinson says. "There are so many things going on at once. Depending on the characteristics of the event, there are usually five or six expensive things that are going to make up the response process."

Price tags vary depending on the nature of the incident—where and how the breach occurred and the number of records affected. The capacity of in-house information-technology and communications staffs also figures heavily in the final bill. Contracting for outside help typically means additional costs starting in the tens of thousands of dollars.

The list of potential expenses is long: consultants, lawyers, call centers, mailings, identity-protection and credit-check services.

"The first thing you might think about is forensics," says Cathy Bates, chief information officer at Appalachian State University and a member of the Higher Education Information Security Council. "Do you have the capability to do it in-house, or will you need to call in forensics expertise? That might be your first outlay of cash. It can be expensive. But again, it really depends on the type of security breach that you are working with."

Timothy P. Ryan, managing director of the cyber-investigations practice at Kroll Inc. and a former FBI agent, says he has worked on some forensics investigations at colleges that were completed in two weeks and others that took months.

Hiring an outside forensics team to investigate a small breach can be done for "under $50,000," he says, with costs for larger incidents escalating from there.

Data breaches in higher education cost colleges an average of $111 per record—a figure that calculates in the damage to the institution's reputation—according to a 2013 study published by the Ponemon Institute, which studies cybersecurity and data protection. The average per-record cost across industries including government, health care, and retail is $136, the study found. Titled "2013 Cost of Data Breach Study: Global Analysis," the report included 277 organizations in nine countries and focused on breaches involving 1,000 to 100,000 records.

"There are probably a lot of data breaches in higher education that go undetected, probably more so than in other industries," says Larry Ponemon, founder and chairman of the institute. "The universities are not aware of data leakage and the harm that can result. It can cost universities a lot of money."

Indiana University has spent about $75,000 on an information call center since officials announced its security lapse, says a spokesman, Mark Land. The university also spent about $6,200 mailing notifications to 6,200 affected people for whom it did not have email addresses. Staff time spent on the security lapse has totaled about 700 hours, Mr. Land says. The university does not budget for potential data breaches and does not have cybersecurity insurance, he adds.

"While this will end up costing the university from a financial standpoint, our biggest concern is making sure we do everything we can to answer questions and to provide support for those affected by the potential data exposure," he says, "and to ensure that we strengthen our processes so that this sort of thing does not happen again.".

Linda Donlin at North Dakota University says the forensics investigation there was done at no cost to the university by the Multi-State Information Sharing and Analysis Center, which serves state, local, tribal, and territorial governments. The university system is spending about $200,000 on identity-theft protection services and a call center, she says.

Costs related to data-security lapses dating to 2011 at the Maricopa County Community College District, in Arizona, could climb to $17.1-million, says Tom Gariepy, a district spokesman. Trustees have approved contracts including $2.25-million for Oracle to repair the network, up to $2.7-million in legal expenses, and up to $7-million for notification and credit-monitoring services, among other costs. He also confirms that the district has received notice of a class-action lawsuit.

BREACHES KEPT MUM

High-profile data breaches cost institutions more than dollars and cents, according to college officials and data-security experts. There are also what some describe as "opportunity losses" and "reputational costs." These can include the embarrassment of having to explain an incident to parents, alumni, trustees, and prospective students.

Mr. Ryan, the Kroll investigator, notes that in many states, reporting requirements center on credit-card, health-care, and personally identifiable information. Cases involving theft of research and intellectual property by foreign hackers are often kept mum, he says.

The public hears of no more than about half of all data breaches that occur at colleges and universities in the United States, Mr. Ryan estimates.

> **"Public exposure for a high-profile breach helps elevate the conversation out of the IT group and into the executive level."**

"When it comes to higher education, a lot of it is reputation," says Mr. Ryan. "The Ivy Leagues have a certain reputation to maintain. If they are besieged by a number of breaches, there is a loss of reputation there. For the same reason schools want winning sports teams, they don't want to be that school that is constantly getting breached."

Cynthia J. Larose, an attorney in Boston with the firm Mintz Levin who advises colleges on data-security-breach compliance and response, says reputational costs are real but hard to pin down.

"It is probably much harder for institutions of higher ed to quantify than it is for retailers, because retailers can see it in their stock price, they can see it in their sales," Ms. Larose says. "Target can directly track a drop in fourth-quarter sales," she says, referring to a case in which hackers accessed as many as 40 million debit-card and credit-card accounts used in the retailer's transactions from November 27 to December 15, 2013.

"Will enrollment drop at the University of Maryland because of this?" she says of the recent breach there. "I kind of doubt it. The alumni-fund-raising office might see a downturn in giving—I don't know. That would be an interesting metric to track."

KEEPING COSTS DOWN

Cybersecurity insurance is both expensive and hard to get, says Ms. Bates, of Appalachian State.

"The experience that I have had a couple of times in working with insurance companies that offer cyberinsurance is that they have a checklist of what you need to show you have in place with your security practices," she says.

"Very often you have to have such a strong security posture before you can even be allowed to get the insurance that it would take you a lot of work on your part to be able to even be eligible."

She does see many colleges working to build in-house forensics expertise, or to establish channels through which to reach out and get it quickly should the need arise.

One way to keep costs down is to have standing relationships and contracts with service companies that can be activated if an incident occurs, Ms. Bates says, noting that many colleges and universities already have such arrangements in place.

As much as they keep those responsible for colleges' data security up at night, news of significant data breaches can help information-technology and data-security officials make their case with top administrators and trustees.

"It can't be a conversation that is led by the IT department, and too often it is," says Joseph Krause, a managing director at Coalfire Systems Inc., an information-technology-security firm that works with higher-education clients.

"So this kind of notice, this kind of public exposure for a high-profile breach, helps elevate the conversation out of the IT group and into the executive level and into the boardroom."

Those working on data-security issues in higher education say they have a particularly challenging task in preserving the open, accessible culture characteristic of the American university while also establishing strong security.

They expect to see more headlines in the coming months like the ones out of Maryland. The problem of data breaches in higher education, many say, is likely to get worse.

"Higher ed is an active target," Ms. Bates says.

"It is not like people are accidentally happening upon us. They are actively pursuing us and trying to get our data."

"I think all of us are actively looking at ways to not only be preventive but to deal with this in the best possible way that we can," she says. "You feel the weight of the whole situation your shoulders. You really want to try and create the best outcome you can for anyone who may be impacted, as well as for the university." ■