Out of the Breach and into the Fire

Two of the entries on the long list of data breaches in higher education are Georgetown University and UCLA. Timothy Lance recently talked with the IT policy officers at these two institutions to identify some of the policy implications of handling data breaches.

Timothy Lance: The incidents at Georgetown and at UCLA were quite different.

Heidi Wachs: Yes: Georgetown's breach involved approximately 38,000 individuals and was due to the theft of an external hard drive. UCLA's breach involved just over 800,000 individuals and was caused by a malicious intruder hacking into its systems. Yet there are many core activities in breach response that are the same and many parallels in the lessons learned.

Kent Wada: The size of our breach held implications for our response. Making a decision about notifying would affect a lot of people. In terms of logistics, we faced several challenges, such as how to send out hundreds of thousands of e-mails without being blocked by major ISPs because we looked like spammers and how to handle the 1,000 calls per hour that initially came into our call center.

Lance: How does handling a data breach differ from handling a standard security incident?

Wada: State data-breach notification laws add a separate dimension to what most standard security incident-response teams already do. Forensics may have to be more formal. Decisions will often require executive authority, legal counsel, and a public relations interface. Execution of notification may require an entirely separate administrative team.

Wachs: Many typical security events are detected by technology or IT department personnel. However, some data breaches will arise differently. For example, if a laptop is stolen, the theft will likely be reported by the device's owner; or if PII [personally identifiable information] is inadvertently exposed on the network, the news media may call to say that a data leak was found through Google's indexing and caching.

Wada: Something to keep in mind even in the midst of a crisis is internal communications in light of possible litigation after the fact. We all depend on the asynchronous convenience of e-mail for work; but we also all know that e-mail communication is very informal, especially in a crisis. Everyone needs to understand when it is appropriate to invoke attorney-client privilege and how to do so. And public institutions need to be mindful of state public records laws that are designed to ensure transparency and accountability, so that they do not inadvertently compromise security-sensitive information that could be used as a blueprint to attack institutional systems (e.g., the exact configuration of an intrusion-detection system).

Lance: Let's focus for a moment on how you decide to notify.

Wada: Notification must be thought through before a crisis hits. In a situation where a laptop with PII is stolen, the notification process is straightforward: the data is in unauthorized hands, and notification is necessary.

Wachs: That's assuming you know what data was actually on the laptop. Accurate inventories of PII must be conducted before a crisis strikes. Georgetown recently approved an “Interim Policy on the Use, Collection, and Retention of Social Security Numbers,” just one of the tools we are now using to conduct a thorough inventory of where our PII is used, stored, accessed, and transferred.

Wada: Unfortunately, the stolen laptop scenario is the easy one. It's not uncommon to be in a situation where the forensics provide only a best/educated-guess scenario, which was the case with the UCLA breach. This moves beyond legal requirements and into the realm of an institution's policy and cultural expectations—that is, which way to err? If an institution chooses not to notify, and later people who weren't notified were among those whose data was exposed, there would be, at the least, reputational consequences. But notifying when doing so is not required can cause unnecessary alarm. UCLA chose broader notification than was strictly legally required.

The University of California uses three sets of factors to make such decisions. The primary criteria speak to the “simple” situations. For example, is it known that the data is in the physical possession of an unauthorized party? The secondary criteria are used when the facts aren't so straightforward. For how long was the data exposed? Has any data, whether PII or not, been copied? Finally, the third set of criteria apply in the most complicated situations. Would it do more harm to notify incorrectly or to not notify correctly? What is the likelihood of fraud or identity theft? In general, the more
ambiguous the situation, the greater is the need to notify.

Wachs: The best thing you can do is uncover the facts to the extent possible, decide what you are going to do based on those facts, and document your line of reasoning; in other words, do due diligence. And use good log-management practices, which will maximize the chance that forensics will result in conclusive facts should a breach occur.

Lance: Once you’ve decided to notify, then what?

Wachs: Notifying affected individuals requires many potential ancillary activities, such as creating a website, setting up a call center, and developing comprehensive messaging both for the internal campus community and for the media. The logistics of notification can be daunting: for example, coordinating with the U.S. Post Office to send out thousands or hundreds of thousands of pieces of mail. A small breach may require only a toll-free phone number staffed in-house, but a larger breach means finding and contracting with a call center vendor with thousands of operators who require precise scripting and the on-the-spot ability to revise based on calls. Georgetown used a call center and also a hotline at the Office of Advancement. In addition, we offered credit-monitoring services for one year, a choice that institutions must consider. The EDUCAUSE/Internet2 Computer and Network Security Task Force’s data incident notification toolkit is a good place to start.

Wada: There’s an important timing issue here. You want to notify as quickly as possible once you have the facts. Often, you won’t yet have all of the facts, but waiting too long can give the perception that the institution is trying to hide something. On the other hand, notifying too quickly means that new information may require further notifications. In addition, if law enforcement is involved, they may request a delay in making a public announcement until their investigation has reached a certain point. Finally, the response package consisting of the call center, a website, and readiness for inquiries must be in place before notification; not having these items prepared is certain to increase confusion and anger.

Wachs: At least forty-three states have separate state data-breach notification laws. Many of them have similar requirements; however, it’s best to work with your counsel to determine how to comply.

Lance: There’s always an aftermath …

Wachs: A Data Security Task Force was formed at the request of Georgetown University President John J. DeGioia. Co-chaired by the university’s Senior Vice President and the university’s Vice President for Information Services and Chief Information Officer, the Steering Committee is composed of key data stakeholders throughout the university including CFOs, vice presidents, and a representative from the Office of University Counsel. The Data Security Task Force is charged with taking a comprehensive look at the university’s critical business, academic, and research functions that utilize confidential and protected data and implementing practical changes to more securely conduct this work. In addition, the Task Force has the authority to approve interim policies in this area. Currently, all members of the university community using SSNs are undergoing an evaluation by me, in the capacity of University Information Services Privacy Officer, in collaboration with the University Information Security Officer and the Office of University Counsel.

Wada: UCLA has an Advisory Board on Privacy and Data Protection, composed of senior faculty and administrators and reporting to the Executive Vice Chancellor, and a Data Council, composed of representatives of the major data stewards and data consumers on campus. The Advisory Board considers broad principles and the application of these principles to new situations in research, education, and administration, whereas the Data Council looks at institutional data-stewardship issues.

After our breach, we had discussions with the California attorney general and members of the state legislature. A College and University Social Security Number Task Force has been created to examine the use of and practices around SSNs and to make recommendations for enhancements. After doing some extensive analysis, we confirmed that we are required to keep most of the SSNs we have now because they are required by external agencies, notably the IRS but also the National Student Clearinghouse, among others.

Wachs: In the meantime, Congress continues to consider several efforts to legislate uniform notification requirements for data breaches.

Wada: And on January 1, 2008, California amended its notification law so that the law is triggered by unauthorized exposure not just of SSNs, driver’s license numbers, and financial account information but also of medical information and health insurance information. Overlap with HIPAA requirements must now be considered as well. But doing so is worth the price, considering the potentially devastating effects of medical identity theft. It’s no longer just your credit rating at stake—it’s your life.

Notes

Heidi Wachs is Director of IT Policy and Privacy Officer at Georgetown University. Kent Wada is Director, IT Strategic Policy, at the University of California, Los Angeles (UCLA). Timothy Lance, President and Chair of NYSERNet (New York State Education and Research Network) and Distinguished Service Professor at the University at Albany, is Editor of the EDUCAUSE Review Policy@edu department.