Data Breaches in Higher Education: From Concern to Action

Data breaches that potentially expose personal information are of great concern to every U.S. citizen and consumer. In August 2007, as reported in The Wired Campus, the Privacy Rights Clearinghouse documented the total number of compromised private records during the past three years at almost 160 million. The Wired Campus article, which noted that many of these breaches had occurred at colleges and universities, concluded by asking: “When is higher education going to get serious about safeguarding the private information of students, faculty, and staff?”

The Chronology of Data Breaches as recorded by the Privacy Rights Clearinghouse (http://www.privacyrights.org/ar/ChronDataBreaches.htm) shines light on this question and on the problems of data security. It does identify higher education as a sector where much work remains to be done. However, the Chronology also reveals that from January to late August 2007, the records compromised at institutions of higher education accounted for less than 2 percent (896,349) of the total number of records compromised during that time. The other 98 percent of breaches occurred in private industry, financial institutions, medical institutions, and other sectors.

What may be confusing is that higher education ranks second in the number of reported instances in 2007 (56), behind government entities (63). In fact, that number represents 25 percent of the reported instances in 2007, a significant decline from the nearly 50 percent level during 2005-6. Other sectors that reported instances of data breaches in 2007 include private industry (49), medical institutions (33), financial institutions (14), and K-12 schools (11). Don’t get me wrong: nearly 900,000 exposed records are too many, and data security must receive more attention at colleges and universities. Nonetheless, it is clear that data compromises are not concentrated in colleges and universities; they are a national problem that affects all sectors of the economy.

In addition, it is likely that breaches in other sectors, especially the commercial sector, are substantially under-reported. Institutions of higher education are highly motivated to report, not only because the financial and legal consequences are less severe than for private companies but also because the academic sense of openness has motivated those in colleges and universities to view voluntary reporting as the “right thing to do”—even before state laws made disclosure mandatory. In states without such laws, colleges and universities adopted cybersecurity and disclosure practices from peer institutions in other states. This is not to criticize other sectors, where the financial issues are significant (one company’s stock plummeted 10 percent five days after a breach was reported in the media), but merely to point out that what makes higher education a target—a sense of openness—is also what motivates colleges and universities to err on the side of disclosure.

There are other factors at play as well: institutions of higher education are technologically sophisticated. With widespread adoption of incident-detection systems and other forensic techniques, academic security staff run more and more powerful tools to discover intrusions, often resulting in the additional need to disclose data compromises that, in other sectors, may have gone undiscovered.

Finally, we should not lose sight of the fact that data breaches also occur with physical “paper” records. It is likely that these breaches are substantially under-reported, as evidenced by an apparent trend in the 2007 list of breaches (e.g., RadioShack’s disclosure that it found twenty boxes of discarded records, including sales receipts with credit card numbers, in a dumpster).

Let me reiterate: academic institutions, like other sectors, have a lot of work to do. The security of private information, computer systems, and campus networks is a major concern, and we must continue to improve awareness and expand technical safeguards. That is why the EDUCAUSE/Internet2 Computer and Network Security Task Force (http://www.educause.edu/security) has been working, since 2000, to organize the higher education community, promote effective practices and solutions, facilitate information sharing, and raise awareness regarding cybersecurity risks. That is why, early in 2007, the Task Force rolled out a “Confidential Data Handling Blueprint” (http://connect.educause.edu/library/abstract/ConfidentialDataHand/44417) and a series of one-day regional seminars on the topic. And that is why the annual EDU-
CAUSE/Internet2 Security Professionals Conference (http://www.educause.edu/securityconference) continues to showcase effective practices and solutions for data security. It is this very philosophy of openness and sharing of effective practices that has allowed smaller institutions and those with fewer resources to work with and learn from larger institutions, making everybody safer.

According to a 2006 study of IT security in higher education by the EDUCAUSE Center for Applied Research (ECAR): “Respondents reported extraordinary changes in both hard and soft security measures.” The ECAR study concluded: (1) “Overall, respondents feel more secure today than two years ago despite being in a perceived riskier environment”; and (2) “respondents from institutions with IT security plans in place characterize their IT security programs as more successful and feel more secure today.”

Colleges and universities pride themselves on their open environments. They also take information security very seriously and have implemented bold steps to improve their practices. These steps are public, visible, and represent the best of higher education—bringing together technical experts, policymakers, and security researchers in colleges and universities, government, and industry. All of us in higher education must continue to work hard to minimize the risks incurred by individuals who entrust us with their personal information, but we must continue to do so in an environment of openness that benefits everyone.

Notes

Peter M. Siegel is Chief Information Officer at the University of California at Davis and co-chair (with Amelia A. Tyanan of Tufts University) of the EDUCAUSE/Internet2 Computer and Network Security Task Force.