

Damage Control: When Your Security Incident Hits the 6 O'Clock News

Even carefully deployed security systems aren't 100% safe. While we work to reduce security exposures, we must also prepare for the day an incident hits the headlines. One way to prepare is to study the lessons learned by those who have "Been there, done that!" This session features three panelists discussing what worked, what didn't, surprises encountered, and surviving the crisis. Below are resources provided by the panelists concerning IT security incidents at colleges and universities.

Georgia Tech

In March 2003, online hackers accessed the Robert Ferst Center for the Arts Box Office computer server. The hackers downloaded information stored on the server as part of the Center's ticket ordering process. Stolen information included names, addresses, phone numbers, email addresses, and credit card numbers.

- Ferst Center for the Arts Box Office: "New Security Measures Protect Your Information": <http://www.ferstcenter.gatech.edu/boxoffice/security.php>
- Internal Auditing (IA) & Office of Information Technology (OIT) Information Security Collaboration Model: <http://www.audit.gatech.edu/IAcollabrative2.wmf>
 - This diagram illustrates how IA and OIT identify, process, and resolve security incidents at Georgia Tech.
- Patron Services Information & Updates: <http://www.gatech.edu/patron-services/>

University of Texas at Austin

In March 2003, a security breach was discovered in a UT administrative database, resulting in unauthorized access to roughly 50,000 names and social security numbers of students, staff, and others. A criminal complaint was filed against a student at UT Austin. According to a statement from the U.S. Attorney, "At this point, there is no indication that the stolen data was further disseminated or used to anyone's detriment."

- Data Theft Incident Response: <https://www.utexas.edu/datatheft/>
- Statement from the U.S. Attorney (March 14, 2003): <https://www.utexas.edu/datatheft/usao-complaint.html>
- What is being done to protect Social Security number privacy at the University?: <https://www.utexas.edu/datatheft/ssnprivacy.html>

University of Kansas (KU)

In January 2003, a security breach was discovered resulting in unauthorized access to the University of Kansas Student and Exchange Visitor Information System (SEVIS) database. Personal information on 1,450 foreign students, including social security numbers, birth dates, passport numbers, and countries of origin was copied.

- KU News Release: <http://www.ur.ku.edu/News/03N/JanNews/Jan22/sevis.html>
- Letter to the International Students Affected by the Computer Hacking Incident: <http://www.ku.edu/identity/letter.shtml>
- Protecting Your Identity: Responding to Possible Identity Theft: <http://www.ku.edu/identity/>

This event is brought to you by the EDUCAUSE/Internet2 Computer and Network Security Task Force. For more information about the Task Force and its projects, upcoming security events, or resources, please visit: <http://www.educause.edu/security>.