Incident Response: Lessons Learned from Georgia Tech, the University of Montana, and The University of Texas at Austin

Judith A. Pirani, Sheep Pond Associates and ECAR

ECAR Case Study 7, 2003
Incident Response:
Lessons Learned from Georgia Tech,
the University of Montana,
and The University of Texas at Austin
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

The mission of the EDUCAUSE Center for Applied Research is to foster better decision making by conducting and disseminating research and analysis about the role and implications of information technology in higher education. ECAR will systematically address many of the challenges brought more sharply into focus by information technologies.

Copyright 2003 EDUCAUSE. All rights reserved. This ECAR case study is proprietary and intended for use only by subscribers and those who have purchased this study. Reproduction, or distribution of ECAR case studies to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior written permission is granted by EDUCAUSE. Requests for permission to reprint or distribute should be sent to ecar@educause.edu.
Preface

The EDUCAUSE Center for Applied Research (ECAR) produces research to promote effective decisions regarding the selection, development, deployment, management, socialization, and use of information technologies in higher education. ECAR research includes

- research bulletins—short summary analyses of key information technology (IT) issues;
- research studies—in-depth applied research on complex and consequential technologies and practices; and
- case studies—institution-specific reports designed to exemplify important themes, trends, and experiences in the management of IT investments and activities.

In its most recent research, ECAR has investigated the state of security practice in higher education and reported its findings in Information Technology Security: Governance, Strategy, and Practice in Higher Education. This research was conducted by a team of researchers from ECAR and from Cap Gemini Ernst & Young. It was undertaken in five phases, described below.

Literature Review

A review of the relevant literature helped us define the study’s major elements and create a working set of hypotheses.

Consultation

Researchers consulted with higher education security and policy leaders to identify and validate the most interesting research questions and hypotheses for framing the construction of a quantitative survey instrument. Those consulted include Mark Bruhn of Indiana University, Ken Klingenstein of Internet2, Mark Luker and Rodney Peterson of EDUCAUSE, Dan Updegrove of The University of Texas at Austin, and Gordon Wishon of the University of Notre Dame. The resulting research framework formed the basis for creation of an online survey.

Online Survey

ECAR conducted an online survey of more than 1,600 colleges and universities to establish the current state of computer security practices in higher education. More than 400 colleges and universities responded to the survey.
Telephone Interviews
Researchers conducted intensive telephone interviews with more than 30 IT and functional executives, managers, and security officers at more than 20 selected EDUCAUSE institutions.

Case Studies
Researchers conducted in-depth studies of institutions regarding the state of their security efforts. To adequately capture the depth and breadth of practice, ECAR researchers chose both public and private institutions that varied in size and mission.

We undertook the present case study to draw on the direct experience of those able to provide insights into policies, technologies, and practices that have worked well and those that haven’t. We assume readers of this case study will also read the primary study, which provides a general context for the individual case study findings.

ECAR wishes to thank Ray Ford, associate vice president for information technology and chief information officer at the University of Montana; John Mullin, chief information officer, associate vice president, and associate vice provost for information technology at Georgia Tech; and Dan Updegrove, vice president for information technology at The University of Texas at Austin, for sharing their time, thoughts, insights, and records with us.

Introduction
Higher education institutions deploy numerous security tools to protect their information technology (IT) operations’ integrity. Despite their best efforts, security is not infallible—breaches do occur. The results of the 2003 ECAR survey on IT security in higher education suggest that some institutions may be insufficiently prepared for an increasingly likely IT security breach. Only 45 percent of responding institutions reported having a formal procedure in place to handle an IT security incident. Incident response, however, “becomes more critical with the ever-growing direct and indirect cost for each occurrence,” stated John Mullin, chief information officer, associate vice president, and associate vice provost for information technology at Georgia Tech. “Certainly you can quantify the direct costs of a security incident—auditing, equipment, and software costs. But we have indirect costs, too—reputation costs and the hidden missed-opportunity and diverted-staff costs. When we looked at the thousands of staff hours that we put into our incident, it was extremely expensive.”

Nineteen percent of ECAR survey respondents reported having an incident newsworthy enough to merit reporting in the press. The risk of negative press coverage, of course, adds another layer of complexity to the incident-response process. Those responsible for IT security at an institution that finds itself suddenly in the spotlight during a difficult time face an uncomfortable and unfamiliar challenge. When handled correctly, such experiences also present an opportunity to minimize any resulting reputation damage and can even raise awareness of complex solutions that often require broad community engagement.

This good-news, bad-news paradox is the crux of incident-response management. While the incident itself can range in impact from an unpleasant nuisance to a potentially expensive and even explosive event, the aftermath does present an opportunity for an institution to improve its operations. The key is to manage the response in an organized fashion: a timely response followed by a thorough incident investigation to identify areas for improvement. A formal plan facilitates the process and is generally considered good practice. At some institutions, as this case study shows, an effective web of in-
Institutional relationships and understandings can somewhat compensate for the lack of formal plans.

Georgia Tech, the University of Montana, and The University of Texas at Austin have all experienced highly publicized IT security incidents. Though each institution's incident-response organization is unique, this case study highlights common lessons and insights that readers can apply to their own institutions. It first acquaints readers with a basic overview of the incident-response process and then reviews the incident, the institution's response, and the impact on the enterprise. Although each institution's CIO serves as spokesperson for this case study, all three acknowledge the critical role their IT staff members play in incident-response efforts.

Incident Response Primer

Many books and articles cover incident response in detail. This section provides a brief overview to introduce readers to the incident-response process, later exemplified by three institutional profiles. Three broad phases exist for incident response:

- **Thorough preparation beforehand** creates an organizational structure, a set of response policies and procedures, and awareness to ensure that the institution knows how to react when an incident occurs.
- **During the actual response,** the institution diagnoses and addresses the problem and communicates its actions as required.
- **The post-incident analysis** renders recommendations and action items for institutional improvement.

The first step is to involve appropriate administrators in creating a common incident-response strategy. This should define what constitutes a security incident at the institution, determine which areas should handle different aspects of a coordinated response, and specify appropriate response actions. “When you are in the middle of a high-profile security breach, you better have a really good partnership among public affairs, legal affairs, the president's office, and IT,” said Dan Updegrove, vice president for information technology at The University of Texas at Austin. Laying the foundation beforehand facilitates the actual response process and gets buy-in from participating administrators.

An incident-response team evolves out of strategy development. It is “not a dedicated team sitting around, but more like a volunteer fire department, where people have other duties, but when there's an emergency, people respond to it.” The response team provides a central authority to coordinate the response and determine who is in charge and how people will respond. IT, legal affairs, and public relations representatives commonly sit on the team, but it can also include “core members and additional support members, consisting of individuals with specific areas of expertise and skills who can be called upon during the incident handling if needed.”

The next step is to create a set of incident policies and procedures. Each institution may decide the appropriate level of formalization for its incident-response process, but even roughly outlining the procedures is helpful. Formalization helps each team member understand his or her duties and actions. “By creating a specific strategy that states what to prioritize and how to react if an incident does happen ... you can limit the damage done and lower the costs of recovery. By knowing whom to call and what to do next, you can decrease the amount of time it takes to recover and possibly save you and your staff from additional disasters along the way.”

Some guides suggest the creation and distribution of an incident-response operation manual that contains “documents and information relevant to incident handling: contact information, incident report forms, administrative report forms, equipment list,
and checklists." Another suggestion is an incident-response flowchart detailing the process that the team should follow during an incident. It spells out step by step what each part of the security organization needs to do when a breach occurs. While the incident process needs to be flexible in order to handle various kinds of attacks, you won’t want to leave out any of the steps in the diagram. Everyone should know whom to call and what to do in every type of situation.

Other recommended practices include “creating a contact list—a telephone tree with telephone and cell phone numbers—for team members and external resources such as law enforcement. It is advisable to list contacts by job function rather than individual name, thereby reducing the need to maintain the list’s currency in the event of employee turnover. Of course, organizational structures and roles change too, so it is essential to update the contact list. This recommendation also assumes that there is a clear reporting structure in place.” Clarity in roles, function, and reporting lines helps the institution refine its response capabilities and speed and adapt to adverse incidents. It is also wise to designate a “documentarian” on the response team beforehand so that it’s clear who is capturing all the incident-related information when a crisis occurs.

When an incident occurs, diagnosis is the first course of action. Updegrove outlined a quick checklist of items:

- What happened?
- When did it start?
- Is it over?
- How did it happen?
- What might be at risk?
- Can we immediately do anything to mitigate the problem? (This analysis can take five minutes or five days.)
- Were any laws broken?

◆ Were critical data affected?
◆ Are other computers on the campus or elsewhere at risk?

The answers to these questions typically help the incident-response team map out appropriate actions. Communication is essential to keep team members abreast of new developments and to inform senior management and other constituencies as needed.

A post-review process is just as important as preparation, to help identify areas of institutional improvement and to fine-tune the process for next time. “After the resolution of the incident, the team should examine all information regarding the incident handling process and the resolution. The data gathered from the review process would be a valuable tool for the team’s further development. This information will aid in identifying strengths and weaknesses and help clarify further training, skills, manpower, policies, or procedure revisions…. The data gathered during the review process will also guide you in the area of policy and procedure development and revisions.”

Three Institutions’ Incident-Response Experiences

“CSIRTs (computer security incident-response teams) are as unique as the organizations they service, and as a result, no two teams are likely to operate in the exact same manner.” This certainly holds true for the three institutions profiled in this case study. Georgia Tech created a formal and documented set of incident-response policies and procedures three years before its incident. The University of Montana created its procedures as its incident progressed. The University of Texas at Austin falls in the middle—policies and procedures were in place, but perhaps not as formally documented as Georgia Tech’s.
Georgia Tech: Strong Procedures Facilitate Incident Response

Located in Atlanta, Georgia Tech is a doctoral research institution with colleges in architecture, engineering, sciences, computing, management, and liberal arts. It currently enrolls 16,500 students and employs 700 faculty members. In fiscal 2001, Georgia Tech received more than $237 million in research awards.

On 14 March 2003, Georgia Tech’s anomaly-based intrusion detection system picked up questionable activity from a server located in the Ferst Center for the Performing Arts. The server stores ticket ordering information: credit card numbers, names, addresses, phone numbers, and e-mail addresses. Further investigation revealed that a hacker had compromised the server, risking unauthorized access to 57,000 theater patrons’ personal information. The locally maintained server was not protected by a firewall, nor was its security software recently updated.

Georgia Tech was thoroughly prepared to address the incident. Of the three institutions interviewed, Georgia Tech has the most formalized incident-response policy. It evolved from an effort three years ago by various academic, research, and business units to create a campus computer network user policy. The Department of Auditing and the Office of Information Technology (OIT) worked together to develop the incident-response team and policies. The flowchart in Figure 1 (prepared by GIT–Internal Auditing) documents the procedures and illustrates specific actions resulting from incident events.

Georgia Tech also created an executive response team consisting of the CIO, the director of internal audit, the director of information security, the director of financial services, the vice president of human resources, the executive director of institute communications and public affairs, the legal counsel, and the director of campus security. The dean of computing didn’t participate in this incident but has since agreed to advise the team. The head of the affected unit, the vice president of student affairs, joined the team during the incident.

The server’s potential compromise coupled with the sensitive information it stored initiated the incident response. The executive
response team convened to discuss strategy. As Georgia Tech’s John Mullin explained, “Diagnosis is a multitrack process. The initial incident reports determine what branches to pursue, and then we start multiple, parallel tracks. Some tracks peter out, others gain importance. The team meets as needed. In this case it was at least daily, sometimes twice daily, to debrief and to evolve our course of action. We briefed senior members of the institution throughout the process.”

Mullin outlined four areas that were active throughout the incident-response process.

- **Law enforcement.** Determine whether to contact law enforcement agencies, including the local police, the Georgia Bureau of Investigation, the FBI, and/or the Secret Service. In this case, Georgia Tech notified all of the above as well as the banks and the four major credit card companies—American Express, Discover, MasterCard, and Visa. Georgia Tech’s information security team has worked hard to develop a close relationship with the law enforcement agencies above, and the effort paid off with respectful and rapid cooperation for this incident. Law enforcement later traced the credit card information to the Dominican Republic.

- **Forensic.** Isolate the asset and protect it for forensic activity, taking into account law enforcement needs. Further evaluation showed the hacker accessed the database but didn’t necessarily copy the personal information. Georgia Tech decided to err on the conservative side and assume that the database was compromised.

- **Communications.** Determine whether the incident might require communication outside the institution, to the press, to students and alumni, or others. Media relations played an important role in the incident response. “I believe our strong, fact-based, open, and frequent communication with the media enabled us to get accurate (nonsensational) coverage throughout the process,” Mullin said. “This didn’t happen by accident.” Georgia Tech also mailed a letter to each Ferst Center patron who had transacted with the system since 1998. The letter explained about the compromised database and patrons’ potential risk for identity theft and fraud, and it provided information for patrons’ self-protection, for example, directing them to fraud alerts at the credit reporting agencies. The message emphasized that no evidence existed about illegal usage. Georgia Tech also established a hot line to answer patrons’ questions.

- **Business process.** Implement required actions to get the affected asset operational—in this case, the Ferst Center’s ticketing system. The OIT instituted several ticketing security measures. A new ticketing process server now resides in a centrally managed, physically secure environment, behind a firewall that restricts access on the basis of IP address and port number. The server requires user authentication and restricts access to certain ticket software functions by user ID. Box office workstations that access the server have personal firewalls and require user authentication, too. The server uses up-to-date intrusion software. Ticket transactions are encrypted, and the credit card number is deleted from the record once the transaction is completed.

One particularly thorny area for Georgia Tech was compliance with Visa’s Cardholder Information Security Program (CISP). After the incident, Visa threatened to pull Georgia Tech’s credit card processing. Because the university’s credit card operations had been compromised, Georgia Tech submitted corrective action plans to satisfy Visa’s CISP requirements for organizations to change their business practices (see the sidebar). “It is well intended in spirit,” stated Mullin, “but it is quite difficult to achieve compliance.”
Visa Cardholder Information Security Program

The Visa U.S.A. Cardholder Information Security Program (CISP, <http://usa.visa.com/business/merchants/cisp_index.html>) defines a standard of due care and enforcement for protecting sensitive information. Because the payment industry places a high priority on maintaining the confidentiality and integrity of account and personal data, CISP requirements are directed to all entities that store, process, or transmit cardholder information. The program ensures the annual validation of merchants and all service providers on both the issuing and acquiring sides of the business.

CISP Requirements

- Install and maintain a working firewall to protect data.
- Keep security patches up to date.
- Protect stored data.
- Encrypt data sent across public networks.
- Use and regularly update antivirus software.
- Restrict access by “need to know.”
- Assign unique ID to each person with computer access.
- Don’t use vendor-supplied defaults for passwords and security parameters.
- Track all access to data by unique ID.
- Regularly test security systems and processes.
- Implement and maintain an information security policy.
- Restrict physical access to data.

Georgia Tech next turned to the incident’s longer-term implications. OIT’s first order of business was to ensure campus security. It surveyed all servers, locating many unprotected devices that contained sensitive information including credit card numbers and information protected under the Health Insurance Portability and Accountability Act, the Family Educational Rights and Privacy Act, and other legislation. OIT is reviewing all these servers but took immediate action in some areas. For example, OIT now centrally manages all credit card processing systems in the campus data center, which offers a technically and physically secure environment.

The university reviewed policies and procedures in two areas directly affected by the Ferst Center security breach: sensitive-information storage and credit card processing. It recently released two new policies. The first requires CIO sign-off before installing servers that store sensitive information. A mandatory preapproval process examines a server’s environment, administration, maintenance, and other business practices to ensure its current and ongoing security. Second, Mullin and the vice president of financial services overhauled the university’s credit card processing activities, creating a two-part review process. One reviews the business process: information collection, accounting, business processes, and electronic information storage. The other addresses the technology systems that support the business process. “We realized a relationship existed between both areas,” Mullin explained. “Issues like data access and data retention are both intertwined.”

With new policies and procedures come education and awareness issues. Institutional response has been positive because many Ferst Center patrons are members of the
Georgia Tech community. “It is amazing how important security becomes when it is your name, address, phone number, and credit card number hanging out in the wind,” Mullin said. “Security became personal; it was no longer a concept. The cultural acceptance is high even though there are significant business process changes.” To educate the university, the campus newspaper has published several articles, and OIT has launched a series of campus meetings with administrators, members of individual colleges, and students (in student orientations), and it has conducted faculty/student-focused town hall meetings.

“The good news is that if an incident does not kill you, it makes you stronger,” said Mullin. “We had a good security program in place, as evidenced by the fact that the breach was self-discovered. However, it highlighted the need for changes in our business processes and practices.”

University of Montana: Forensic Work Strikes the Right Balance

The University of Montana, located in Missoula, Montana, is a doctoral institution with more than $50 million in research activity annually. The university’s seven schools train students in journalism, law, business, forestry, education, pharmacy, and the fine arts. The university’s College of Technology offers courses in 25 programs, including retail management, electronics, and practical nursing. Current student enrollment exceeds 12,000, and the university employs almost 800 full- and part-time faculty members.

The University of Montana’s incident stemmed from a mistake, not a malicious act. A valid user with an authorized account for Web postings on a university-hosted dot-org site inadvertently uploaded the contents of a personal PC hard drive to a university account. The more than 6,000 files uploaded contained e-mail, digital photographs, and other personal items, as well as confidential clinical psychology files. All 6,000 files were unrelated to the University of Montana but accidentally appeared on the institution’s Web site and were accessible only through the Web site’s indexing mechanism, not directly.

On 5 November 2001, someone discovered the files and tipped off the press. Then Ray Ford, associate vice president for information technology and chief information officer at the University of Montana, experienced every CIO’s worst nightmare: the public relations office received an unexpected phone call from a local television station. The reporter described the confidential files posted on the university’s Web site, outlined the station’s plans to run the story, and notified the office that a news reporter would arrive in about a half hour to interview a university representative.

The University of Montana had no formal incident-response policy, but the press call initiated a chain of events: a call to the university attorney, a call to Ford, and Ford’s call to the director of the computer center to secure the Web site. After a quick consultation—and without his input—the university named Ford the incident spokesperson. Fortunately, Ford’s previous experience in security issues as a consultant for the U.S. Department of Defense helped him define the university’s incident response.

The IT department deleted the files from the Web site immediately upon determining they had been saved correctly for the incident postmortem. “I tasked the director of the computer center with securing the confidential information on the Web site,” stated Ford. “It is not as easy as just deleting things. You need to do it carefully—in a way where the files are inaccessible, but also so the information and the logs are intact to do a careful postmortem.” The university also created a team to respond to the incident; it consisted of the CIO, the computer center director, two psychology department representatives, and the university attorney.
Ford realized from the outset that each file, and even the file name, could contain sensitive data, so he restricted access to the logs and the files. He created “silod” investigative tracks to minimize the accidental spread of confidential information. As the primary spokesperson, Ford did not view either the logs or the files, to avoid inadvertent exposure of confidential information to the press. The university attorney handled any multi-institutional concerns, accessing detailed information only when circumstances dictated. The computer director accessed only information logs for forensic activities, using the Web site's indexing log to carefully study who accessed what file and in what order. The university’s psychology department representatives reviewed the 6,000 files’ actual content. Their three-month investigation determined that the files were not associated with any university activities and identified which files contained potentially confidential information.

“At that point the two streams merged. We cross-checked the potentially confidential files with the log of accessed files. We ended up with a small set of files that were confidential and accessed,” Ford said. After reviewing the IP addresses, the IT department determined circumstantially that some people received links to confidential files in the query results to Choices, the university’s fringe benefit package. The links appeared so far down in the list of query results that most people did not access the files. Two people, however, did, and within minutes after their sessions’ termination, people with IP addresses traced to news organizations started similar queries. Ford speculates that some university insiders may have tipped the news media. Most of the files were not accessed even though they were available for viewing. Upon completion of the investigation, Ford released a report to the press and other interested parties about the IT department’s findings.

“This incident has raised the issue of IT security on campus,” stated Ford. “It is certainly ironic, because the incident had nothing to do with the hackers or break-ins that you spend all this money to prevent. But it has gotten us a sympathetic ear.”

The university’s post-incident activities focus mainly on enhancing its Web operations. When the incident occurred, budget cuts had left several Web positions empty, including the Web director position. The university has since centralized its Web operations, hiring a Web director and developing a mandatory online training program about Web content contributors’ rights and responsibilities, with recertification every six months. The training program is a collaborative process with all university constituencies. The Web director is coordinating the training, but she worked with stakeholders on the course’s design and content.

The university has strengthened its Web policies, too, giving a single person within an area Web-posting responsibility and instituting more stringent policies regarding dot-org Web site hosting on University of Montana servers—something authorized only for approved university programs. Some university departments are investigating the feasibility of moving and centralizing their Web server operations. Ford wants to investigate content management options, too.

However, Ford realizes that the same incident could occur tomorrow, even with stricter policies. “Unless we conduct a lengthy and careful review of all the material that is posted on our Web, the best we can do is to train the people who are empowered to post information on the university Web site and hope they don’t make a mistake,” he explained. “This is an academic institution. We will not implement a mandatory review of all postings. So the big policy change we lobbied for was the training and the recertification of the training.”
Finally, the University of Montana is developing a formal incident-response procedure to handle the next press call. Current procedures govern how a union employee reports a suspected IT security breach, partly because university system administrators are union employees. Ford, however, wants to document the entire process. “We have bits and pieces,” he said, “but we are working on drawing everything together.”

“When I talk about the incident at conferences, one slide thanks the free press,” said Ford. “It is not the first thing that comes to mind after spending literally days talking to reporters. I would have preferred if the tipsters called me directly, but the media alerted us just in time. If the exposure continued much longer, we would have received more hits than we could track. But the bottom line is that this can happen to anybody. That is the chord that really resonates with IT managers when I talk to them.”

The University of Texas at Austin: Experience and Policy Go Hand-in-Hand

With an enrollment of more than 52,000 students, The University of Texas at Austin is the flagship institution of The University of Texas System and the largest campus in the nation. The institution employs approximately 3,000 faculty and 18,000 staff, offering more than 100 undergraduate degree programs and 170 graduate degree programs in eight colleges and seven schools. UT Austin annually receives more than $300 million in research grants and contracts.

UT Austin’s incident occurred on a seemingly minor mainframe-based system that managed employee training classes. Employees used the system to register for classes, and managers used it to review their staff’s training histories. Both accessed the system using the university ID number, which has for many years been the individual’s Social Security number (SSN).

On Wednesday, 26 February 2003, the Information Technology Services staff responded to a system crash in the Web front end but incorrectly attributed the anomaly to faulty testing during a recent software upgrade. On Sunday evening, 2 March, a system administrator observed unusually heavy activity on the system, all originating off campus, and disabled the system. Subsequent system log analysis indicated that the system had received more than two million queries over five days from two separate IP addresses, with roughly 50,000 names and SSNs exposed.

The training system vulnerability evolved from a series of seemingly unrelated decisions. The compromised system was built not as an enterprise-wide production system but as a quick-and-dirty way for administrative systems staff to manage internal training program participation. “The application lacked data input checking, since it would be used only by a few trusted staff, and it benefited from the implicit ‘security by obscurity’ of an IBM 3270 interface and its mainframe operating system,” explained Dan Updegrove of UT Austin.

Decisions made several years later compromised this security by obscurity, however. To save time and money, the university decided to use this application when it needed a generalized training compliance system. To improve ease of use, it added a Web interface with security provided by the authentication built into the UT Austin portal. Later, another UT campus requested and received unauthenticated access to the system to avoid having to register all their staff in the UT Austin authentication process.

“Any one of these decisions was potentially benign,” stated Updegrove. Taken together, they created a serious vulnerability.

UT Austin’s policy is to report any suspected problems related to data or network security—illegal behavior, viruses, rogue traffic, and so on—to the central Information Technology Services staff.
Security Office, which has formal interfaces to the rest of the UT Austin community, including departmental IT units, legal affairs, public affairs, the UT Police Department, and the UT System Office of General Counsel. “We don’t have a cookbook—if x, then y,” Updegrove said. “But the key points are that, first, everyone on campus knows about the Information Security Office. Second, the Information Security Office reports directly to a vice president. Third, I can call upon essentially any resources that I need anywhere on campus…. It is incredibly important to have a process in place so the incident does not get submerged three or four levels deep in the IT organization.”

That Monday morning, UT Austin launched a systematic response to the security breach. The response team’s immediate task was to review all administrative systems for similar exposures, and it found none. Needless to say, the team also permanently closed the training system’s backdoor interface.

Next came diagnostics. The team traced the attack to two cable modem customer addresses, one in Austin and one in Houston. While waiting for the required subpoena to ascertain the customers’ names, IT staff members reviewed other logs to determine whether the offending IP addresses had been used to access other systems requiring authenticated login. When IP addresses matched, the university had strong circumstantial evidence identifying the perpetrator. “Not all hackers are geniuses,” Updegrove said. “Being able to write a Perl script to exploit a system’s vulnerability doesn’t require deep knowledge of network architecture. Hackers think they are anonymous, not realizing they are leaving tracks in the system logs.”

Quick thinking also contained further damage. When the response team found that one person—an Austin resident—was using the two separate IP addresses, it created a strategy to try to “recapture” the data before they could be disseminated or misused. That is, if the computer(s) could be confiscated quickly, the risk to the individuals named in the stolen data could be mitigated. UT Austin worked with law enforcement officials, who quickly served a search warrant to confiscate the computers and materials less than three days after the breach was discovered. “It appears we succeeded,” Updegrove said. “I don’t know if we will ever be able to prove it, but the good news is that in four months, we are not aware of any systematic misuse of the data.” The U.S. Attorney’s Office filed charges against the student on 14 March 2003, and the case is still pending at this writing.

With the incident under control, attention turned to notifying all affected individuals. “The decision to notify affected individuals posed an ethical quandary. This frankly is a whole domain that I never gave much thought to: what obligation do you have to your patrons and customers? Given the paranoia about identity theft, how do you get this out in a responsible way that does not create more panic? There is a question of moral versus legal obligations to notify people if their records have been exposed,” Updegrove explained. “We had no legal obligation to notify anyone, but we felt a strong moral obligation to do so.”

The university used two primary communication modes. The IT department had created a Web site (http://www.utexas.edu/datatheft/) earlier to inform the public about the incident, coincident with the initial press coverage. People could access the site and contact the university directly with their current mail or e-mail addresses. UT Austin also sought to mail a letter to each affected individual, alerting the recipient to the data theft and providing identity theft protection recommendations, including referrals to the three major credit bureaus’ free fraud-alert services. “By asking people to sign up for the fraud alert, we hoped they would inform us if their data were being misused,” said Updegrove.
The mailing turned into an arduous task because so many of the database's addresses—for former students, faculty, staff, admissions applicants, job applicants, and so on—were outdated. When letters were returned as undeliverable, the university contracted with third-party address database companies. Language was another, and unanticipated, problem. UT Austin sent the first mailing in English, but not all people associated with the university are native English speakers. As a result, information was posted in both English and Spanish on the incident Web site.

Interestingly, UT Austin has not reached closure on the attack, because the federal case is pending and the defendant has not been made available to be interviewed. Thus, uncertainty remains as to how the attacker discovered the security vulnerability. Nevertheless, Updegrove plans to weave security more tightly into application system design and testing, with the assistance of a newly hired analyst in the Information Security Office.

“The incident’s irony is that last year we charged a task force with designing a plan to replace Social Security numbers as the university ID,” stated Updegrove. “We realized that careless use of Social Security numbers could cause problems outside the university. Unfortunately, we were only part way into the process when the security breach occurred. This incident obviously redoubled our interest in creating a new university ID.” Updegrove estimated the incident’s cost to date as exceeding $120,000 for printing, mailing, toll-free hot line charges, third-party address databases, and staff time.

“We did a lot of soul searching on how we got into that particular situation,” he said. “As is the case with most post-incident analyses, it was not one little thing, but multiple errors, that created the problem. We were victimized by a whole succession of ‘John did not know what Jane did.’ Assumptions were made that were not true.”

**Incident Response Best Practices**

Upon reviewing the incidents, several effective practices emerged from the three institutions’ incident-response actions.

**Strong Preparation Affects the Entire Response Process**

Both Georgia Tech and UT Austin had created incident management policies beforehand, which guided actions during their incidents. The policies specified response teams that convened quickly and which, in turn, determined an appropriate course of action. Georgia Tech’s flowchart provides a handy reference tool by graphically illustrating the process. Working with other team members may also facilitate post-incident improvement. Coincidentally or not, Mullin and the vice president of financial services, both members of Georgia Tech’s executive response team, worked together to revise credit card processing procedures after the Ferst Center incident. At the minimum, their participation on the same incident-response team gave them a running start on their project.

**Communication Is Key**

All three institutions communicated frequently during and after their incidents to report their progress to the public and to inform affected constituencies as needed about potential information exposure. The University of Montana conducted numerous press interviews and engaged all affected areas of the university in the design of its new Web content training program. Georgia Tech’s executive response team communicated regularly with senior management. Georgia Tech and UT Austin mailed letters to affected individuals. Georgia Tech has embarked on a university-wide education
program about upcoming policy changes. UT Austin created a dedicated Web page to communicate the latest incident developments and to enable concerned individuals to contact them.

Determine Appropriate Information Access

The University of Montana’s Ford recognized quickly his incident’s delicate nature. The inadvertent exposure of the uploaded clinical psychology files or file names recorded in the logs during the post-incident analysis could compound an already sensitive situation. By using siloed investigative tracks, he ensured that no one had access to all the information, thus decreasing any potential exposure.

Leverage the Incident for Institutional Improvement

Georgia Tech and the University of Montana used their respective incidents to improve operations in their impacted areas. The incident enabled the University of Montana to draw attention to the lack of management in its Web operations. Both institutions created new policies to tighten any procedural loopholes.

Experience Counts

Experience—or the lack thereof—played an important role in the UT Austin incident. An inexperienced system administrator may have delayed the initial incident determination, but the UT response team’s experience resolved the crisis quickly. They instinctively knew to cross-check IP addresses among various logs to identify the attacker, and to engage quickly with external law enforcement for subpoenas and search warrants. At the University of Montana, Ford drew upon his experience with the defense industry when formulating his response strategy.

Lessons Learned

Ford, Mullin, and Updegrove all cited several lessons that any institution can apply to its incident-response strategies. The lessons match the three incident-response phases: preparation, response, and post-incident analysis.

Preparation

◆ We are all in this together.
According to UT Austin's Updegrove, effective incident response expands beyond IT’s borders. "It served us enormously to have a very sophisticated public affairs office that had good relations with the press and a legal affairs office that understands information technology. They quickly grasped the problem and its many dimensions. We all worked together to create a systematic response."

Response

◆ Honesty is the best policy.
UT Austin’s reputation may have been damaged when the press reported the data theft, but good communication minimized the long-term damage. Updegrove observed, “I think being forthright served us well. We took a fair amount of heat, but our constant communication demonstrated our commitment to address the problem. A number of people said our candor and honesty were refreshing and rare.”
◆ Law enforcement involvement is good and bad.
Although an institution loses control when law enforcement enters the response process, such involvement is a potent public relations tool. “Once you engage law enforcement, they own the process, the timing, everything,” Updegrove explained. “Having them respond forcefully and aggressively reassured the public that we aimed a lot of expertise and firepower at this problem. UT Austin was not hiding anything.” For example, UT Austin
posted statements from the U.S. Attorney on their incident Web site.

- **There are two sides to every story.**
  When the Austin American Statesman ran its news story, it publicized the UT incident Web page address. According to Updegrove, “We had no idea how the story would play out, but we knew it would receive lots of attention. A URL in the story enabled us to publicize our side of the story instantaneously, which became extremely valuable when the story hit the national news wire. It enabled us to be proactive, too—updating the story in real time and enabling people to address us directly with their concerns.”

- **Slow and steady wins the race.**
  Rather than racing to conclusions, the University of Montana’s incident postmortem lasted several months to thoroughly investigate the incident without compromising sensitive information. According to Ford, “We were very careful about how we handled the postmortem. Some parents were particularly anxious for an answer, but each time I talked to them, they seemed more and more responsive. They understood that we were doing our best, and simple, quick answers were not what we and they wanted.”

- **Reporters are not technologists.**
  Both UT Austin’s Updegrove and Montana’s Ford found that reporters seem to absorb some technical facts more readily than others. Updegrove found that reporters leaped from a data-theft incident to an identify-theft incident in the space of a few sentences. Ford found that reporters considered the incident to be a University of Montana problem, even though the user uploaded files onto a dot-org site hosted by the university. According to Ford, “If it is in your domain, reporters consider it your responsibility, no matter who actually operates the site or server in question.”

**Post-Incident**

- **A strong offense is a good defense.**
  After the Ferst Center incident at Georgia Tech, Mullin found that his periodic briefings about incident management helped senior administrators recognize the incident’s true causes. “Because I apprised senior management regularly about our incident management policy and awareness activities, they immediately recognized the incident resulted from a lack of compliance, not a lack of policy,” he observed. “This enabled the whole team to focus their efforts on the response.”

- **Talk is good.**
  Some institutions might try to sweep a widely publicized IT security incident under the rug as quickly as possible to minimize reputation damage. Yet all three institutions have talked frankly about their incidents to educate others. According to Montana’s Ford, “At my CUMREC and EDUCAUSE presentations, audience members commented on my bravery to talk about the incident in public, but both the university president and attorney encouraged me to give the presentation. This incident is not going away. The Chronicle of Higher Education still references it occasionally. I want to explain how a similar incident could happen to others, and I assert that any institution’s similar experience might be of interest to others.”

**Conclusion**

Institutions should not overlook incident response in their overall IT operations, because “knowing how to respond to a security incident—be it a computer worm, mistake, hacker, or the mere suspicion of a problem—can save [an institution] time, money, and even its reputation.” Georgia Tech’s Mullin concurred. “Incident-response policies are tools to help you to deal with the incident more effectively and more quickly. We weren’t paralyzed when the incident occurred. After you get past the expletives, you have a process to follow. We tune it for the next round and we hope we never need it—just like insurance.”
Endnotes

1. The scope of the security study was based on ISO/IEC 17799:2000, including system access control, system development and maintenance, compliance, personnel security, security organization, computer and operations management, asset classification and control, and security policy and its deployment, and excluding business continuity planning or disaster recovery and physical security.

2. Although this survey was not randomized or stratified, creating the risk of both survey and respondent bias, it was universal for research universities and oversampled both M.A. and B.A. Carnegie institutions. The data reflect very closely the general EDUCAUSE membership, including the relatively smaller participation of A.A. institutions.


6. Ibid.

7. Ibid.

8. Ibid.


11. S.D. Scalet, op. cit.