

Academic Computing Vulnerabilities: Another View of the Roof

A faculty-driven audit offers a complementary perspective on network disaster planning

By **Ellen R. Cohn, George Klinzing, Irene Hanson Frieze, Susan M. Sereika, Clement A. Stone, and Clara M. Vana**

"The time to repair the roof is when the sun is shining." —John F. Kennedy

President Kennedy's 40-year-old quotation is as timely as ever when applied to academic network failures. In anticipation of Y2K, and later as a result of heightened security concerns following the events of September 11, 2001, numerous colleges and universities developed formal planning documents to guide their responses to unexpected network outages.

Typically, vigilant institutional financial auditors or information technology directors initiate campus-wide crisis planning efforts. The University of Pittsburgh similarly maintains an updated Y2K-derived plan, and, like many academic institutions, enjoys a reliable and stable computing environment. Recognizing, however, that unanticipated network outages can seriously interrupt business functions, the university also initiated a faculty-driven audit to identify the potential effects of network failures on academic functions.

As a result of what we learned from this initiative, we suggest that other institutions may similarly benefit from integrating two complementary approaches to network disaster planning.

The Challenge

The University of Pittsburgh's Computing Services and Systems Development (CSSD) provides computing support, development services, telecom-

munication services, and the information infrastructure necessary to the educational, research, and administrative activities of students, faculty, and staff. CSSD also provides significant and ongoing support to individual units, a commitment articulated in the university's technology plan:

The existing departmental support model recognizes the need for centralized and distributed information technology resources to support the implementation of technology-related initiatives throughout the university. Departments receive assistance through the services of the Help Desk, Contract Support, Training Services, and the Expert Partners programs.¹

The challenge arises as follows. At the University of Pittsburgh, as is typical for large research universities with multiple campuses, schools, departments, and centers, it is not unusual for local units to hire and maintain their own IT staff and establish local servers to run specialized computing labs, departmental research, and other functions. This has resulted in many local IT configurations (some in geographically distant locations), each with a need to fully protect essential business functions to avoid costly system failures. Thus, like many universities, we were faced with a computing architecture that appeared to require an additional, complementary approach to self-study.

The challenge of systems disaster plan-

ning for an amalgamation of central and localized academic computing infrastructures is analogous to crisis management planning for public roads that span a large metropolitan area, with federal, state, county, and local governments each maintaining its respective roadway. The stakes become high when the economic vitality of the larger region is unexpectedly threatened by unrecognized vulnerabilities within critically situated local roadways. The same interdependencies may occur within large university systems. Each of these environments requires a high degree of internal information sharing and coordination to anticipate and manage emergencies.

There are also cultural challenges inherent in any academic system. Both the business of universities and supporting information systems occur in juxtaposition with academic cultures that have evolved over hundreds of years, research-based imperatives that drive institutional excellence, and a competitive admissions marketplace. Thus, critical timing factors unique to academic institutions, if subject to disruption, can cause expensive business losses. For example, system failures at inopportune times could prevent completion of multi-million dollar grant applications, disrupt and even negate time-dependent research protocols, and prevent prospective graduate students from submitting deadline-dependent electronic applications. While these major issues were obvious to all, upon

further discussion we began to discern less obvious vulnerabilities that we needed to take into account.

Indeed, systems disaster plans may not reveal the subtleties of academic computing vulnerabilities within each of the diverse units of a large research university. Why might such be the case for plans developed with university-wide representation? It is natural for planning efforts to focus on central technical functions—how system-wide outages might occur, be prevented, and/or be corrected. The brightest beams shine on the largest systemic vulnerabilities for valid reasons: in the absence of back-up systems, a power outage in a major university computing facility could have far-reaching negative consequences. Therefore, centrally driven plans must concentrate on “the big picture.”

Extending President Kennedy’s example, we must first view “the roof” from above. Yet, if called upon, those inhabitants of academic subunits who live beneath the roof will likely be able to contribute new and valuable information. They will be able to uniquely identify what parts of their local computing infrastructures system are the most vulnerable to disruptions and identify where “leaks in their roof” could result in the most serious damage.

The Process

The University of Pittsburgh decided to initiate a faculty-driven audit to more fully discern the potential effects of network failures on academic functions. Before this process was initiated, the university considered the costs and benefits of several approaches.

Approaches Considered and Rejected

The first option proposed was to engage a consultant to audit local academic computing environments. This was deemed an unnecessary expense given the available internal expertise.

A second option was to ask the director of CSSD to assign members of that staff to conduct an audit. This option was rejected so as not to divert that staff from their specialized functions when other options existed.

A third option was to seek the assistance of the Expert Partners Program, a group of systems analysts and other information technologists who supply computing support on the local level. The Expert Partners Program

...was developed to provide assistance to departments with support personnel responsible for providing day-to-day computing support. The program is devoted to building strong, positive relations between central and departmental support staff by providing in-depth access to technical resources. Individuals participating in the program have access to electronic resources, technical meetings, a Web site with technical information and links, a group discussion area, and an array of training for applications and University network services.²

While many in the Expert Partners group were ultimately called on to contribute to the reports, we decided that a faculty-initiated project would most fully assemble the nuances related to customers’ perceptions of academic computing.

Approach Chosen

The concept of an academically driven audit process emerged from faculty discussions in the provost’s Council on Academic Computing (CAC),³ a committee chaired by the vice provost for research. The CAC was established in December 1999 “to provide guidance to the Provost regarding academic computing issues; specifically by recommending priorities and policies, and reviewing proposals in the areas of network services, acquisition of instructional software, and development of specialized facilities.”

The committee consists of 23 faculty members, most appointed by their deans. Committee members represent the arts and sciences (3); health sciences (5); professional schools (6); and regional campuses (6). In addition, faculty members serve from the university senate’s Computer Usage Committee (2), and the committee includes the director of CSSD. The CAC is led by a tenured faculty member who is a high-level

administrator in the provost’s office.

The CAC meets monthly to foster intra-organizational communication, seek new opportunities, recommend policy, and engage in problem solving. The CAC maintains ad hoc working subcommittees, which in 2002–2003 included the high-performance network computing initiative, faculty training, the future of academic computing, and the faculty portal.

In 2001, the Subcommittee on Systems Failures was formed within the CAC. The group was charged to detail instances of past and potential network computing disruptions across mission-critical academic units at the University of Pittsburgh.

At the request of the associate vice provost who serves as the CAC chair, the deans and directors of major academic units each identified an individual within their organizations who could describe the effects of interruptions in network computing. We also invited the participation of a number of non-academic units (for example, the office of undergraduate admissions and financial aid and the office of the registrar), selected because of their functional impact on the academic mission of the university. (See the sidebar for the letter of invitation to participate.)

The interview procedure was as follows. Five faculty members from the subcommittee conducted interviews at a total of 25 sites, ranging in size from very small units to regional campuses. Forty-seven respondents provided information. Interviewees variously consisted of administrative staff, computing staff, faculty, and high-level administrators. Some individuals spoke solely from their own perceptions, while others sought pre-interview data from a representation of their colleagues and/or furnished a prepared summary approved by administrative leaders.

The interviews focused on the types and functional (specifically, business) effects of network computing disruptions and did not dwell on the technical aspects of the disruptions. Interviews ranged between 30 minutes and two hours and, unless otherwise noted, were conducted onsite between March and

May 2001. The interviews were conversational and open-ended, with the intent of eliciting the content most pertinent to each site.

Each interviewer submitted a written narrative. These were edited and summarized by the subcommittee chair and assembled into a report presented to CAC, CSSD, and the university provost. Three major outcomes of the audit—new information, common themes, and local introspection and change—are described below.

New Information

The elicited scenarios yielded as a primary outcome a rich body of new information concerning potential vulnerabilities. The process provided all concerned with a greater appreciation of the ways in which mission-critical university functions could be vulnerable to computing failures.

The process also stimulated dialogue and valuable mutual learning among local administrators, faculty members, and IT staff. This created an enhanced understanding of their mutual dependencies on technology. Six examples follow.

School-Based, Research-Related Services

■ *Grant preparation and submission.* One unit perceived vulnerability to disruption: "The capability to process and submit research grants on a dated basis is often network dependent. The school processes 10–15 grants each day. These include NIH [National Institutes of Health] and NSF [National Science Foundation] submissions. Loss of the capability to complete a grant might result in loss of many months of work, loss of reputation with collaborators from other institutions, and loss of potential funding. Files housed on a UNA [ubiquitous network access] platform are especially vulnerable."

Another unit perceived less vulnerability: "Systems disruptions would cause minimal disturbance to ongoing research. For clinical research studies, many databases are housed on individual instruments or on local

servers. Submission to NSF, for example, might be delayed by network outages; however, the school is aware of alternative submission strategies if needed."

■ *Computational functions.* "Research dependent on computational capabilities would be delayed, and even potentially adversely affected by network outages. For data sent to the Supercomputing Center, calculations may take several days. Network interruptions might result in lost and/or delayed calculations."

■ *Research, journal, and conference participation.* "Electronically conveyed time-dated applications and reviews might be disadvantaged by network failure. There is apparently no computational interaction with the Supercomputing Center. One faculty member relies upon the network to accomplish data mining."

School-Based Student Services

■ *Graduating student placement.* "The placement process is highly dependent on the Internet and e-mail. Approximately 250 graduating students compete nationally for jobs. Pitt network failures would delay their ability to learn of and respond in a timely and competitive manner to job offers."

■ *Online admissions.* "Applicants who prefer to apply online would be unable to do so."

International Services

■ *Communication.* "Several faculty members (within the school) travel to Brazil and Prague to teach. E-mail is an important source of internationally based communication."

Health Sciences Services for Clinical Rotations

■ *Access to patient records.* "Systems interruptions that prevent access to patient records profoundly affect both research and students in clinical rotations."

■ *Student/sponsor communication.* "Both e-mail and the Blackboard [Web-based course management] systems are key to communicating with preceptors who sponsor students for clinical rotations."

Customer Services

■ *General student services.* "A system-wide disruption would prevent creation of ID cards, processing of housing requests, the ability to enter housing contracts, and the assessment of damages/payments. Registration and transcripts would not be processed."

■ *Financial aid.* "Our office would virtually be shut down if there were outages. We process all financial aid via the Web. This means that students would not have aid credited to their bills, loans could not be processed, and we could not receive reimbursement from the federal government. Information could not be accessed concerning a student's financial account."

Regional Campus Services

■ *Academic functions in the humanities.* "For classes, students who have papers due could not turn them in on time; frequently, their excuses are legitimate. Instructors who use Blackboard and online materials would be greatly affected. The fine arts classes are a perfect example. The graphics program doesn't operate when the network is down, so the instructor is unable to make a fast switch to using slides, etc. In effect, the instructor comes to class well prepared in the high tech world and has little or no advance time to go back into the cave—slides, handouts, etc. Deadlines for creating, printing, and proofreading materials, especially for schedules, theatre and music department programs, important announcements, and so forth, are suddenly way off deadline."

Common Themes

The resultant report yielded a second outcome, the following common themes expressed throughout the interviews.

Potential Types of Disruption

The subcommittee identified numerous types of potential disruptions:

■ Service disruptions to customers stemming from an inability to access the databases to respond to their queries, accept their payments, or respond to their e-mails

- Server-related functions (for example, files and applications)
- Recruiting, applications, and admissions
- Advising
- Purchasing
- Financial services
- External e-mail
- Computing labs that rely on university networking
- Research (data analysis, submissions, and communications with collaborators)
- On-campus Web-based teaching and instruction
- Distance education
- Web sites
- Library
- Student computing in the dormitories
- Clinical documentation and scheduling for units that serve patients

Potential Business Losses

Most units related potential business losses secondary to systems interruptions. The resultant “costs” could variously affect the institution, its workforce, and its customers (for example, students, alumni, and community-based employers). Three distinct categories of loss emerged:

1. *Undetectable costs.* Losses that generally would be incurred as a result of “the store’s not being open” when “customers” are most disposed to apply for admission, enroll, or hire a graduating student cannot be measured. E-mails not received—with no way to alert the sender or recipient—resulting in potential loss of reputation (individual, suggesting non-responsiveness, or institutional, suggesting system instability or unreliability) would fall into this category.
2. *Deferred loss recovery.* Most known losses would be recoverable given a short window of interruption (one to two days). These loss types would include class registration, access to Blackboard Web-based software and distance-education testing, clients not promptly serviced in the law clinics, library research, and file share. It is important to note, however, that negative effects of the disruptions would also extend to the “catch-up” periods following the disruptions,

when faculty, staff, and students must work harder or longer, or defer or neglect other tasks, to get back on schedule.

3. *Human costs.* Some units reported that interruptions could cause substantial stress and aggravation. The estimated amount of stress described related to the potential costs (for example, missing a large research grant submission) as well as public reaction (for example, hundreds of students lined up for many hours, unable to be served). Individual personality differences and employee job functions influenced perceived stress levels. The unpredictability of the interruptions also added to stress levels, as well as not knowing how long the interruption might last. Effective communication during a loss—addressing what happened and why, how and when the problem will be resolved, and efforts to ensure that it won’t happen again—seemed to reduce the stress for some. In addition, promoting alternative strategies—such as working on a non-network-dependent task or replacing a PowerPoint lecture with an in-class activity—helped reduce stress levels.

Timing Factors

Two major aspects of timing emerged:

1. *Critical deadlines.* Admissions or financial aid deadlines, research grant or paper submissions, data analysis for active research protocols, end-of-semester testing, and conference registration would all pose greater challenges and reduced opportunities to recover losses.
2. *Length of outage.* Some university units indicated that interruptions beyond one to two days would be devastating, while other units seemed better able to sustain function over time.

Localized Back-Up Systems

It became clear that there was a wide variability in dependence on the university computing network, even within individual units. Some units had unique computing dependencies, as in the School of Medicine for resident “matches,” the School of Law for con-

nections to downtown courts, and the School of Dentistry for patient scheduling. Some units maintained IT architectures that were less dependent on the university network; these appeared to have evolved for reasons other than protection from network failures.

Local Introspection and Change

A third major outcome was that various units engaged in intra-organizational reflection concerning their dependencies on computing network functions. Units identified new areas of vulnerability and ways to avoid network-related losses. Some stated that specific changes would follow, such as the installation of localized back-up systems.

Issues ranged from realizing that a Web site wasn’t routinely backed up to discussing when a system’s shutdown would most affect critical business functions such as admissions deadlines, research grant submissions, and class registration.

The interview process thus appeared to stimulate thinking concerning business continuity issues.

Relevance to Other Academic Institutions

This project could be relevant to other academic institutions in several ways:

- It presents a structure for a university-wide committee on academic computing, in which faculty members work together within subcommittees to explore potential opportunities and challenges.
- Other academic entities may similarly benefit from integrating “audit/IT driven” and “academically driven” approaches to document the potential effects of computing-based systems disasters. Such use of faculty members can obviate the need to pay consulting costs and/or divert IT staff from other responsibilities and generate an audit that incorporates “consumer perspectives.”
- Ongoing dialogue heightens awareness of the impacts of computing systems disasters, which can stimulate individual units in large academic institutions to evolve their computing and

business practices to offset the effects of short-term network disruptions.

Future Directions

The chair of the Council on Academic Computing will revisit the need to focus attention on academic computing vulnerabilities and update the report within the next academic year. In that event, we might consider incorporating the perspectives of another set of customers—students, a key constituency that is likely to yield yet another “view of the roof.” *C*

Acknowledgments

This presentation was featured as a poster session at the EDUCAUSE 2002 Annual Conference in Atlanta, Georgia, which also featured comprehensive audit-driven approaches described by Jay Dominick, Assistant Vice President, Information Systems, and Chief Information Officer, Wake Forest University.

Endnotes

1. See the University of Pittsburgh technology plan at <<http://technology.pitt.edu/itplan/>>.
2. Find more information on the Expert Partners Program at <<http://expert.cis.pitt.edu/>>.
3. The Council on Academic Computing is explained in more detail at <<http://www.pitt.edu/~vpres/CAC/>>.

Ellen R. Cohn (ecohn@pitt.edu) is Assistant Dean for Instruction, School of Health and Rehabilitation Science, and Associate Professor, Department of Communication Science and Disorders; George Klinzing (klinzing@engrng.pitt.edu) is Associate Provost for Research and Professor, School of Engineering; Irene Hanson Frieze (frieze@pitt.edu) is Professor of Psychology, Business Administration, and Women's Studies, Department of Psychology, Faculty and College of Arts and Sciences; Susan M. Sereika (ssereika@pitt.edu) is Associate Professor, Department of Health and Community Systems, School of Nursing, and Departments of Biostatistics and Epidemiology, Graduate School of Public Health; and Clement A. Stone (cas@pitt.edu) is Associate Professor, Department of Psychology in Education, at the University of Pittsburgh. Clara M. Vana (cva@pitt.edu) is Assistant Director, Millstein Library, University of Pittsburgh at Greensburg.

Invitation to Participate

March 2, 2001

Dear _____,

As our university continues to broaden its use of technology for instruction, communication, research, finance, and infrastructure, our growing reliance on technology increases our vulnerability to system disruptions. While the university has worked hard to supply reliable network connections, as with any service failures can occur.

Provost Maher has charged a subcommittee of the Council on Academic Computing to conduct interviews across all sectors of the university and identify the possible effects of computer network disruptions. You have been identified as an individual who might provide valuable perspectives on the possible effects of network failures on your school or unit.

One of the following committee members will contact you shortly to schedule a 30-minute interview: Ellen Cohn, Irene Frieze, Susan Sereika, Clement Stone, or Clara Vana. Interviews are to be completed by mid-March, and we will very much appreciate your participation.

Some issues you might consider prior to the interview: whatever the causes of system disruptions, the effects can range from minor annoyances to significant losses of function or resources. We are most concerned about technology failures at critical times in mission-sensitive areas. For instance, systems interruptions could potentially:

- Shut down computing laboratories
- Delay electronic submission of student work and grading
- Prevent use of Blackboard and in-classroom Web-based resources
- Deter preparation and/or submission of research proposals
- Interfere with research protocols
- Halt financial/business transactions
- Render UNA machines inoperable
- Result in loss of Web traffic and, thus, potential students

Please consider what technology-dependent functions in your unit are mission-critical and therefore would be most affected by network failures. Rather than present you with specific questions, we will ask you to describe potential scenarios that might ensue if the network were to fail. Prior to the interview feel free to consult with others in your unit to prepare a list of potential problems and their effects.

If you are not contacted for an interview by March 9, kindly inform Ellen Cohn at ecohn@pitt.edu. Again, thank you in advance for your assistance.

Sincerely,

George E. Klinzing
Chair, Council on Academic Computing and Vice Provost for Research