Computer-Related Incidents in Colleges and Universities: 
Factors and Categorization

Presented at the 2004 EDUCAUSE Security Professionals Workshop

May 17, 2004 
Washington, DC

Virginia Rezmierski, Ph.D. 
Adjunct Associate Professor 
CIFAC Principal Investigator 
Gerald R. Ford School of Public Policy and the School of Information 
The University of Michigan 
ver@umich.edu 
734-615-3884

Daniel M. Rothschild, M.A. 
Master of Public Policy Student 
CIFAC Research Assistant 
Gerald R. Ford School of Public Policy 
The University of Michigan 
drothsch@umich.edu 
734-615-9595

© 2004 by the Regents of the University of Michigan. All rights reserved. 
This work is licensed under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.0/ or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.
Previous Research

The Computer Incident Factor Analysis and Categorization Project, or CIFAC, is a research project being undertaken at the Gerald R. Ford School of Public Policy at the University of Michigan. It builds on work previously undertaken by the principal investigator, Virginia Rezmierski, in the ICAMP-I, ICAMP-II, and LAMP projects.

A brief description of these projects is in order. The Incident Cost Analysis and Modeling Project (ICAMP-I) examined ways to measure costs associated with incidents and determine how much incidents were costing colleges and universities. A sample of 30 incidents showed a total cost of $1,015,810, with the cost per incident varying depending on type and scope. This project was followed by ICAMP-II, which sought to evaluate incidents from a risk-management perspective. Smaller incidents were analyzed in light of their frequencies and costs to determine expected costs of each type of incident per annum. A framework was established for evaluating expected costs versus costs of prevention. Finally, the Logging and Monitoring Privacy (LAMP) Project looked at the extent to which system administrators logged and monitored traffic and activity, and examined the legality of this within the framework of FERPA. It concluded that there was inadequate training for IT personnel regarding legal liability issues associated with monitoring and that liability escalates when departments function in isolation.

CIFAC is divided into two sections. The first section, sponsored by EDUCAUSE, is now complete, and this presentation serves to present the conclusions. The full text of the final report is available online. The second section of the project is being undertaken with funding from the National Science Foundation. It is expected to be completed by July 2005.

The questions being asked by CIFAC include:

- How do incidents compare across institutions?
- How do other institutions handle similar incidents?
- What are the causative and facilitative factors associated with different incident types?
- What are the best practices available for incident prevention and management?

The purpose of the first phase of this project was to lay the groundwork for the larger investigation, as well as to examine current practices in incident management, including evaluating common languages for describing incidents. A thorough literature review was conducted of both academic and practical literature. The CIFAC staff conducted three focus groups with college and university incident management professionals in order to gauge current practices and attitudes.
Introduction

Since the purpose of our project was to examine the ways in which IT professionals in higher education thought about and responded to incidents, we began by asking the question: what is an incident? This may seem obvious to everyone; indeed, it seemed obvious to us. But during our review of the literature and through preliminary discussions with practitioners, it became clear that there was indeed no agreed upon definition of what constitutes an incident. Indeed, if you get ten incident handlers in a room together, you are likely to walk out with twenty different definitions of the word. For many, if not most people, their definition of incident is the same as Justice Potter Stewart’s famous definition of obscenity: I know it when I see it.

Is it important to know what incidents are, to have a definition of what an incident is? We believe that it is. Most practitioners have developed a finely tuned sense of what an incident is from years of experience in handling them. Experience is the best teacher, and the visceral reaction that seasoned IT administrators have to various types of incidents provides the best definition available. Unfortunately, we cannot quantify visceral reactions, nor can visceral reactions be shared among colleagues.

It is important to have a definition of what qualifies as an incident because many people involved in the incident prevention and resolution process are not veterans of the IT world. Indeed, many of them have only the vaguest notions of the technical ins and outs of network management, data security, and user intervention. When people from across campus – not just technologists but student affairs staff members, college attorneys, law enforcement officers, students, staff, and faculty – are involved in one form or another in the handling of incidents, it is important that they know exactly what an incident is.

In addition, even among technologists, there may be some disagreement as to what incidents are. Network specialists may tend to have network-centric views of incidents, while data managers may not see a frozen IMAP server as an incident at all. It certainly is an incident, however, from the perspective of the network people as well as the hundreds or thousands of users who cannot access their email.

Frequently, we have found that technologists, especially security professionals, tend to employ a narrow definition of incidents as threats to the integrity of systems or networks. Incidents that affect the continuity or accuracy of data, or those that involve malicious attacks on users often get left out of the scope of incidents. It is important, for reasons that I hope become clear soon, that any institutional definition of incident takes into account all negative risks related to information technology, not just those affecting system stability.

The cause of many incidents does not have a technical fix. Firewalls, high-level encryption, and multiple passwords do not protect a database if just one person with legitimate access has his or her password stolen through social engineering or the all-too-common Post-it-note-on-the-monitor. User education is the only way to prevent something like this, aside from simply turning the server off altogether. In evaluating all the threats to university computing resources, the data they house, and the users that depend on them, it is important to look at every possibility for trouble.
Methodology and Definitions

A brief word about methodology. We convened three focus groups, on each in Chicago, Bloomington Indiana, and Arlington Virginia. We had a total of 33 participants from two dozen institutions participating. Through a series of discussions and written exercises, we gauged participants’ understanding of the seriousness of incidents and the variables that they use in determining how serious incidents are. We owe them a great debt of gratitude for their participation and insight.

In an effort to steer our work and to give our focus groups some common ground, we created our own definition of what an incident is, based on synthesis from existing literature. The definition that we used in our focus groups was:

An incident is an event that utilizes or exploits information technology resources or security flaws therein, either by accident or by design and through malice or otherwise, that causes, directly or indirectly, one or more of the following occurrences:

- Compromise of proprietary, confidential, or protected data,
- System disruption which impedes user(s)’ access to data or other IT resources,
- Violates IT use policies set out and made known by the administrator(s) of the IT systems in question,
- Violates norms commonly accepted within the community of system user(s) for use of IT resources,
- Attempting or conspiring engage or represent oneself or another to be engaged in any aforementioned behavior.

While the overall reaction to our definition was positive, many participants in our focus groups commented that it read like “legalese” and was too unwieldy for practical use by incident response personnel. In retrospect, we completely agree. Based on discussion in these groups, we created another definition that is a bit shorter and easier to use. It is:

An incident is any action/event that takes place through, on, or involving information-technology resources, whether accidental or purposeful, that has the potential to destabilize, violate, or damage, the resources, services, policies, or data of the community or individual members of the community. Such incidents may focus on/target individuals, systems/networks, or data resources and result in a policy, education, disciplinary, or technical action.

We do not suggest that this is the last word on the subject. Indeed, our definition is far from perfect in many regards. However, we wanted to offer a definition that was not solely focused on network security and that was broad enough to encompass the many different ways in which an incident can occur and the different vulnerabilities against which an incident may act. From this, we can start to determine and quantify institutional risk from incidents. We are continuing to refine our definition as we progress into the next stage of research.
Risk-Management Approach to Incident Management

So now that we have a definition, albeit a temporary one, of what an incident is, what purpose does this serve? Our investigation draws on the work of the ICAMP studies, where Dr. Rezmierski was also the principal investigator. ICAMP-II, in particular, laid groundwork on looking at incidents through the lens of benefit-cost analysis. Our intent over the next fourteen months is to extend this concept to determine what factors are associated with or causative of computer-related incidents. This will lead us towards creating a best-practices framework for institutions under which they can undertake their own benefit-cost analyses of potential risks and their consequences.

Why is incident prevention from a true risk management approach important to an institution and, particularly, why is it important to IT professionals? First, it is because incident prevention tends to become solely the responsibility of the IT staff. Incident prevention faces the particular problem of being a negative deliverable. Money and time spent on preventing incidents is seen from the perspective of the unenlightened college administrator as disappearing down a black hole. If incident occurrence is low, it becomes easy for those not involved with IT to assume that the efforts spent are wasted. IT staff do not get praise for preventing incidents, but they do get blame when an incident occurs. If a server freezes, or a virus begins spreading, or a user is being harassed over email, people immediately notice. In my four years of doing first-level tech support, I remember dozens of angry users complaining about various incidents. I don’t remember a single person calling to thank my organization for having had the email servers running smoothly all week.

It is neither fair nor efficient to place the burden for incident prevention solely on IT staff. Incident prevention is everyone’s responsibility. This is not commonly understood, however, and IT specialists have long had difficulty engaging non-technical administrators on security needs. One of the things we are hoping that our final report will do is to demonstrate to non-technical university administrators that incident prevention needs to be a wide-reaching effort. It requires the cooperation and vigilance of all members of the campus community.

The second reason to take on a risk management view of incidents is that it allows for a benefit-cost analysis of what the costs of a potential incident are, versus the costs of preventing it, in light of the expectation that such an incident will occur. In order to do this, IT organizations and personnel have to reflect on their primary mission: supporting the technology needs of the faculty, staff, and students on campus. A benefit-cost analysis has to ask: what will this incident mean to users? Institutional risk managers are particularly well equipped to quantify such risks, with input from the IT department. College attorneys can detail the legal ramifications of a potential incident. Other members of the campus community may be able to contribute to this equation. The bottom line is this: the resources available to preventing incidents are limited. What is the best way in which to deploy them? That is what this next phase of our research hopes to address.

The third reason that a risk management view of incidents benefits IT staff is that it allows for the codification of certain rules of action. In our focus groups, we found a good deal of discussion of a concept of what we call thresholds – certain perceived or actual variables that
automatically trigger a certain response. Ask yourself: what thresholds, if any, exist at your institution? How many users have to be affected, and to what degree, before key people become involved? Are these rules written, or are they just commonly understood? We have found that answers to these questions vary widely.

Thresholds are especially important in cases where there may be legal or public relations ramifications from an incident. For example, in some jurisdictions, the law requires that owner of a database that includes certain private information such as grades or social security numbers notify anybody whose information may have been compromised. Some institutions set up the real or perceived unauthorized penetration of this database as crossing a threshold that requires the involvement of college attorneys, the CIO, the registrar, or other community members. Thresholds should be set by consensus of stakeholders across institutions and made specific to particular institutional needs, with regard to local laws and regulations. Defining thresholds has the important function of establishing what risks the information infrastructure at an institution faces.

From the technologist’s perspective, the benefits of thresholds are twofold. The first reason is that thresholds serve a certain “C.Y.A.” function. If thresholds are determined in advance by stakeholders throughout the institution, and first-responders follow the set protocols for action, their judgment cannot be second-guessed by others with the benefit of 20/20 hindsight. When an incident crosses a prescribed threshold for action, technologists do not have to instantly exercise discretion that will inevitably be second guessed. The second benefit is that technologists can immediately start working on the technical causes of the problem and staunching further damage. In some incident situations where seconds count, not having to spend ten minutes determining who else, if anyone, to involve can make a significant difference to the total institutional cost.

Much of what we have learned or surmised about the necessity of incident management by risk management in a university or college setting is now being written about in the literature regarding the corporate setting. There has been a movement towards a more holistic view of incidents, especially their prevention, that involves managers from throughout a company. There is a maturing perspective on incident management that is more inclusive, wider, and requires greater participation across institutions. Certainly, we have seen this beginning to occur in colleges and universities as well. Robert Austin and Christopher Darby wrote an article in the Harvard Business Review last June that emphasized the role of business managers as well as technical managers in preventing and managing incidents. Their paper is worth quoting at some length here.

Business managers, not just technical managers, are the ones who will have to deal with the consequences of a security breach, which is why they’re the ones who should spearhead preventive measures, and fast.

[The] role [of business managers] should be to assess the business value of their information assets, determine the likelihood that they’ll be compromised, and then tailor a set of risk-abatement processes to particular vulnerabilities…. The goal isn’t to make computer systems completely secure—that’s impossible—but to reduce the business risk to an acceptable level.
It is our belief that the same principle applies in the higher education setting. The difference, as you are all aware, is that faculty and students are not regular employees. They – we – tend to be require more open systems, access to a more diverse collection of resources, and usually cannot be fired for failure to follow rules set out by the IT department. Indeed, we are rewarded for experimentation, and breaking rules in the name of a good cause can be a badge of honor. However, it seems as if the corporate sector and the higher education sector could learn a great deal from one another in the handling, prevention, and management of incidents.

There is one other point that I wish to discuss relevant to our review of the literature that is important to our discussion of what an incident is. Much of the focus of research regarding incidents has been on vulnerabilities, especially those particular to one operating system or protocol, and types of attacks. It is important to note that these are not the same thing as incidents. Attacks are certainly one cause of incidents, but they are far from the only one. Unavoidable hardware failure, social engineering, lack of appropriate policy or failure to enforce policy, lack of physical or virtual security, uneducated users, ignorance of the law, incorrect privileges, and configuration errors are all factors identified by participants in our focus groups as factors that cause or help to cause incidents. Viewing incidents solely as attacks gives a false sense of security and a myopic view of the risks associated with information technology.
Incident Categorization

I would like to shift the focus now to the categorization of incidents. As I have already discussed, when looking at potential incidents from a holistic point of view, it is important to bear in mind that incidents come in many flavors and affect different resources. A network can be locked up as tight as a drum, but one bad user password can bring the whole thing crumbling down. Sensitive data can be kept under high levels of virtual and physical security, but a failed hard drive combined with inadequate backup can render the data irretrievable. Because we have found that incidents can wreak havoc in different sectors, which often have different staffs responsible for related incidents, we would like to discuss some conceptual models of incidents. Different institutions have different levels of communication in this regard. How well do people in your institution communicate about incidents across departments?

This goes in tandem with what we have seen at many colleges and universities. For some time, many college and university IT personnel have kept lists of different types of incidents and kept back-of-the-envelope calculations of how frequently each occurred. These lists do not necessarily imply any relationship between types or hierarchy of incident severity. Indeed, they are nominal lists that do not imply relationships or common causalities. They are simply lists of incident names to allow managers to record and aggregate data. For example, one list includes the following: pornography, hate, denial of service, commercial use, chain letter, copyright, spamming, junk email, unwanted email, mail bomb, commercial spam, allegations of wrong doing, threats, security attack, harassment, stolen/shared password, forgery to conceal identity, privacy, and ping attack. Only a few colleges and universities have begun to categorize or codify computer-related incidents and establish thresholds to trigger appropriate responses. We hope that our conceptual models might help institutions with this task.

The first model we present is the model created by Rezmierski et al in the ICAMP-II report. It distinguishes three types of incident based on the incident focus. The foci are data, users, and operating systems. To clarify, the focus of an incident is the area in which the activity of an incident is based. It is the target of an incident, whether the incident was intentional or unintentional. It was found by the ICAMP-II team that these were the major categories of incident type. That is, they found that all incidents could be sorted neatly into one of these three categories.
In the first phase of CIFAC, we tested this model and expanded upon it. This revised model is another way of looking at the ICAMP-II model. In this model, an incident could be likened to a hurricane. In order for a hurricane to form, surface water must be at least 26.5 degrees Celsius. Air must cool rapidly with respect to changes in altitude. Wind must be going in the right direction. And this must all happen further than 500 kilometers from the equator because of the Coriolis effect. These can all be likened to factors at an incident.
After this incident is formed, it can be empirically categorized into a data, people, or system related incident. Note that these are different terms than were used in the ICAMP model. Here, we replace “user” with “people,” as the focus of an incident affecting your campus may indeed be focused on a person who is not a user. Indeed, an attack on a person thousands of miles away can have ramifications on your campus. In addition, we replace “operating systems” with “systems.” Many incidents that affect systems or networks have nothing to do with a particular OS. Indeed, many if not most system-focused incidents are platform independent. Denial of service attacks, power failures, and cut fiber optic lines are all equal opportunity incidents. Bored teenagers, your local utility company, and campus facilities management don’t care if you’re a Mac OS, Windows, Linux, GNU, BSD, or Amiga OS shop.

After categorization, an incident is rated on several variables that affect perception of urgency to respond. We identified many of these variables, and I will discuss this later. Most of the variables and their rating is something that happens intuitively, and includes questions such as: Is there a risk somebody will be hurt? How many people are affected? How much will this cost the institution? Is there an issue of criminal wrongdoing? These variables may in turn cross thresholds that require some specific action, or they may be at a level that allows individual discretion. Either way, they inform us how to respond, how rapidly to respond, and who should respond to an incident. To bring back my hurricane metaphor, in a hurricane one variable is trajectory. A storm that looks like it’s heading for Miami will definitely trigger a different response than one looking to peter out in the North Atlantic. Similarly, a category five storm triggers a different reaction than a category one – here, wind speed is another variable. Just as trajectory and speed help describe a hurricane, number of people affected and types of data affected help describe an incident, and therefore the proper response.
Currently, we’re working on further refining this model and trying to make it more intuitive. Graphic representation of these concepts is difficult, but we believe it is a useful undertaking in the long run.
Focus Groups

Turning now to evidence gathered in our focus groups, I need to discuss how these models played out when put to the test. One of the experiments we ran in our focus groups was to give each participant a stack of 21 short incident descriptions on three by five index cards. Each incident description was less than sixty words in length. Minimal details were given because we have found that technologists often have to address incidents without knowing many, if any, details. Participants were asked to rate each incident’s seriousness with respect to their urgency for response, and to decide whether the focus of the incident was on data, people, or systems – the three foci in our model.

In all, some 692 incidents were rated and sorted. About thirty seven percent of these were categorized as system incidents, twenty two percent were categorized as data incidents, and forty two percent were categorized as people incidents. We found that there was statistically significant agreement across all three focus groups as to the focus of our 21 incidents. Similarly, there was statistically significant agreement as to the seriousness of incidents. Thus, participants could reliably sort incidents by seriousness and by focus, controlling for variables such as the participants’ jobs and focus group geography. This indicates that the CIFAC model of incident categorization is a solid foundation for discussing incidents across institutions.

In addition to looking at the sorting of incidents, we wanted to see what effect role has on perception of incident seriousness. We say role rather than job title for two reasons. First, many technologists have responsibilities and duties that are not immediately evinced by their job titles. As organizations change, so do the duties of their employees. Frequently, job title is not changed rapidly enough to keep up with it. Second, job titles are frequently broad – such a “technologist” or “research assistant” – that give little indication of what the title holder actually does. Third, the wave of uptitling in the late nineties left many people holding fatter titles instead of fatter paychecks. For all of these reasons, we asked participants to identify what they did most of the time in their jobs rather than what is printed on their business cards.

Our focus group participants fell into thirteen different roles. These included security officer, CIO, network security manager, policy director, compliance officer, and data manager. Our sample sizes in each role ran from one to eleven. Thus, we are short of a statistically significant sample, meaning we cannot evaluate responses by role using statistical methods. However, we can glean some insight about the effect of role on incident perception.

For instance, there was a split regarding which of our short incidents was the most serious. For CIOs, administrators, and policy directors, an incident involving a denial of service attack was seen to be the most serious. For network managers, security directors, and systems administrators, it was an incident involving the unintentional large-scale release of personal information that struck them as most serious. In addition, we saw diversity of opinions by role in our open discussions. Policy directors tended to see educational or policy fixes to problems, while security directors and network administrators more quickly looked to technical solutions. This seems to follow logically, but we are left wondering in what other ways roles influence not just perception of incidents, but the ways in which they are managed. As there seems to be a
correlation between institutional role and perception of seriousness, it seems logical to conclude that the differences in incident perception must create differences in incident management.

Switching away from role, I’d like to address our findings with respect to variables used by our participants in judging the seriousness of incidents. By variables, we mean the questions that participants either explicitly ask themselves or intuitively use to decide how serious an incident is. Variables can be dummy variables: something either is or is not present. They can also be continuous variables: the number of amount of something. Finally, they can be descriptive, unquantifiable variables: adjectives and descriptors that do not translate well into numbers.

We researched this question two ways. First, each participant was given a set of six incident descriptions of between two and three hundred words in length. These were meant to give more background and fully elaborate on details of an incident, both relevant and not. These are our so-called “long incidents.” They were asked to rate the seriousness of each incident on a scale of one to four and then to list and explain which variables or statements within the incident they considered important in evaluating incident seriousness.

Out of the six incidents, two were given mean ratings at a statistically lower level than the other four. That is, to paraphrase Guy Smiley, two of these things are not like the others. This led us to explore what variables might have made the two outlier incidents different than the other four, more consistently rated incidents.

Textual analysis of answers found that three variables caused the disparity between very serious and less serious incidents:

- The first variable is quantity or extent of loss. In the two less serious incidents, there was little actual damage done. One of the incidents was merely a prank, but the other was an attempted intrusion that could have proven quite serious had it gone undetected. It does not seem to be the potential for damage as the actual damage that causes perceptions of seriousness to rise.
- The second variable is the importance, rank, or level of the people involved. Presidents and provosts – those with high rank, especially administrative rank – tend to have incidents affecting them taken more seriously.
- The third variable is the immediacy or need for action due to the potential for further access, damage, or danger. When incidents are retrospective in nature, there is a tendency to downplay their seriousness. When all the facts are in, incidents are judged less harshly than when the next phase of the incident is left to the imagination. We consider this a crucial point: uncertainty can yield action.

We identified fifteen discrete variables in the free response section of the long incident questionnaires. To touch on the most common ones: Far and away, the risk of harm to people – or the lack thereof – was the most commonly cited reason for rating incidents high or low. The risk of physical harm to people seems to be a threshold set across institutional lines. We consider this a good sign: people, not systems, are considered of top importance when looking at incidents.
Potential criminality – violations of FERPA, HIPAA, or other laws – was the next most common variable given. This is probably a result of the fear of litigation under these acts, as well as the DMCA. When participants smelled a potential legal violation, they were quick to comment that attorneys or law enforcement should become involved. This supports the concept of thresholds that are, if not identified in policy, at least part of the general norms of many IT organizations today. Again, criminality seems to be a threshold, which crossing brings in attorneys and the police.

One other variable tied criminality for a joint second plane. That is the assertion that the incident in question is not the job or responsibility of the person giving the rating. This indicates that, as job responsibilities become more specifically defined, incidents that fall outside the scope of individual roles are quickly handed off.

The “not my job” phenomenon is closely tied to a process we call undefining. Undefining occurs when a particular type of incident seems to happen very frequently, such as with spam or harassment. Because of their frequency, they get made “not incidents”; these undefined incidents are often seen as a problem for somebody else, such as student affairs staff or university counsel, and are not a problem for the IT department. Undefining and not-my-job-ism do not reflect poorly on IT personnel. Rather, they speak to the well-recognized but seldom-rectified underfunding of IT security in higher education. Undefining and handing off are necessary coping mechanisms. Without these tools, IT staff would have to spend more hours than there are in a day just addressing incidents.

Two things happen as a result. First, these incidents may not get handed off to the appropriate authority. IT staff are often the first notified about many incidents that may more appropriately be in the portfolio of another campus organization. But without a means of sharing these incidents between organizations – or even within the same distributed IT department – they may fall between the cracks. Second, undefining incidents is directly at odds with a risk-management approach to IT security. As undefined incidents tend not to make it into incident databases, it becomes impossible to truly quantify and assess risk. Regardless of whether these undefined incidents are relatively minor – like spam – or more significant – like a student using a stolen credit card number online – if they are not tracked, thorough risk assessment is not possible.

The other way we tested the variables used to identify the seriousness of incidents was in a more formalized context. Participants were given a list of ten variables, which we selected from the literature, previous research, and comments from professionals in the field. Participants were asked to indicate, out of the ten variables, which five they deemed most significant in influencing their judgments about incident seriousness. These responses were then immediately tabulated, and the four most selected variable from each group were paired against each other.

The results here closely followed the free responses from the long incidents. Probability of danger to person(s) was far and away the most commonly identified variable, followed by type or sensitivity of data, probability of further access or damage, and cost to the department, college, or university. Each percentage listed is the percent of the time that variable was picked as more important than the variable it was paired against.
Causative Factors

The final aspect of our focus group research that we’d like to discuss is the open session about causative factors. You will remember that factors are what create an incident, and than the severity of an incident is a function of how it scores on different variables. This is the main focus of the second phase of the CIFAC project, but we thought a brief, informal discussion with our focus groups might help set us out on the right foot, as well as give some indication as to what factors it is thought are most likely to cause incidents.

We identified seventeen unique factors from the focus group discussions. (Show on screen and discuss each briefly.) Analysis of the responses showed that “user education or lack thereof” was identified most frequently as a causative factor for the incidents that were reviewed. Second to that was “poor or non-existent policy,” followed by “too much or inappropriate access” and “lack of physical security.” We can offer little in the way of concrete conclusions from these discussions, but we can see that user education and the existence of good policy are important factors tied to many incidents in the minds of our respondents.

Tying back into what I was saying earlier, this further demonstrates the importance of a culture where everyone takes part of the responsibility for incident prevention. Setting policy should be done with stakeholders across the institution, and maintaining an atmosphere of responsible use is in turn the obligation of every stakeholder. Incident prevention is everyone’s responsibility, and coordinated education beginning before arrival on campus can significantly reduce the time IT professionals have to spend putting out fires.

The final report from the first phase of CIFAC is available at http://www.educause.edu/asp/doclib/abstract.asp?ID=SEC0409