

Evaluating Computer-Related Incidents on Campus

The CIFAC Project looks at current trends in how incidents are discussed, categorized, and managed

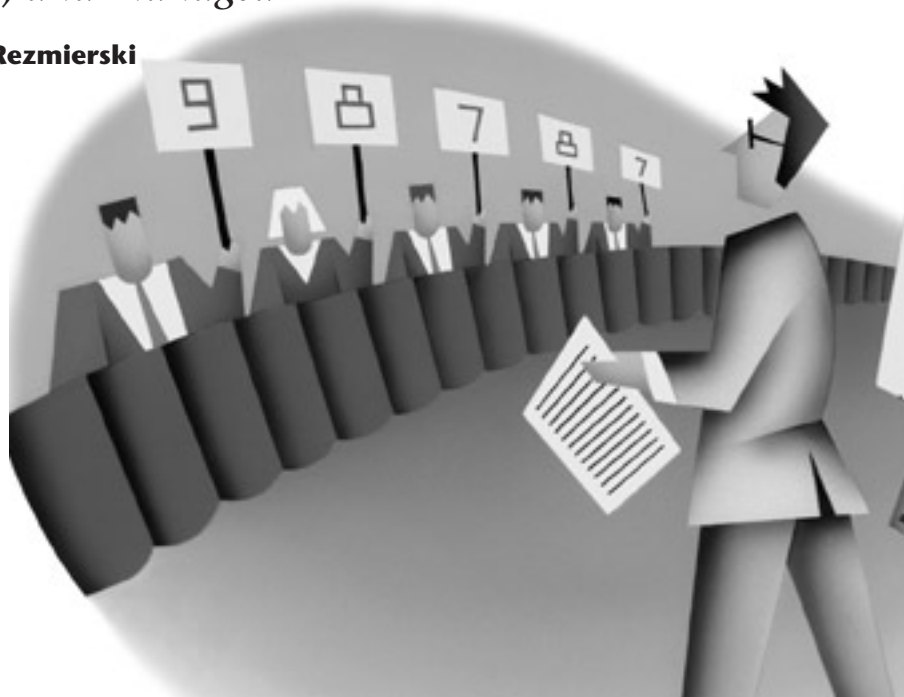
By **Daniel Rothschild** and **Virginia Rezmierski**

The Computer Incident Factor Analysis and Categorization (CIFAC) Project¹ at the University of Michigan began in September 2003 with grants from EDUCAUSE and the National Science Foundation (NSF). The project's primary goal is to create a best-practices security framework for colleges and universities based on rigorous quantitative analysis of high-quality data regarding computer-related incidents.² To this end, project team members are examining factors that cause, encourage, or allow incidents to occur, with an eye to developing a common language with which to discuss incidents.

The CIFAC project consists of two phases: CIFAC-EDUCAUSE, which was completed in April 2004, and CIFAC-NSF, which is currently under way. The CIFAC-EDUCAUSE phase had three objectives:

- Review current literature on incident categorization.
- Harmonize the literature with the ICAMP-II categorization model.³
- Test and discuss our findings and categorization model with higher education incident handlers and security practitioners.

In the CIFAC-NSF phase, we will analyze data collected from 36 colleges and universities and up to 18 corporations and nonprofit organizations to explore factors that allow or contribute to computer-related incidents. We expect to produce our final report by the end of July 2004.



CIFAC-EDUCAUSE: Methodology

We began with a comprehensive review of a wide variety of reports, books, and journals that gave us a broad view of how incidents are discussed and categorized throughout academic, business, nonprofit, and research settings. The goal of this review was to find a means to discuss

- *Types of incidents*: the different focuses of incidents.
- *Incident management*: how to mitigate the ill effects of and stop further damage from an incident.
- *Incident metrics*: the ways in which we measure the seriousness or extent of an incident.

Between November 2003 and January 2004, we conducted three workshops in

different geographical areas, involving a total of 33 computer-incident professionals with 11 different primary job responsibilities from 24 colleges and universities. We intended to explore relationships between how security professionals view incidents and their organizational roles; variables that formed these perceptions; agreement regarding the relative importance of these variables; and any correlation between incident seriousness and incident categorization.

To explore the relationship between role and incident perception, at the beginning of the workshop we asked participants to define their primary role within the university. Over the next roughly four hours, we took participants through a variety of written and oral

activities that gauged their perception of the seriousness of several different incidents and discussed the variables involved in determining seriousness.⁴

CIFAC-EDUCAUSE: Results and Analysis

Although the literature review and workshop activities indicated a growing recognition of the need for a common language to discuss computer-related incidents, we found some trends that we consider detrimental to the establishment of a common language and categorization scheme. Of particular note is a phenomenon we refer to as “undefining”: deciding that certain events should no longer be logged or discussed as incidents. Common examples in the university setting include illegal peer-to-peer file sharing and spam. Because of their frequency, these incidents are being handled either by modifying technical systems or by assuming that the university counsel, student-affairs staff, or another division of the institution will deal with them. Such undefining, however, can skew or cloud our understanding of the full scope of computer-related incidents and thus quantification of institutional risk.

Incident management is increasingly team-based and centered on research and pedagogical needs. The literature showed a rise in modifications to existing approaches to incident prevention and handling. For instance, nontechnical personnel such as student-affairs staff are increasingly likely to be involved in the prevention and resolution of incidents. We found an increasing awareness that technical fixes to human problems are unwise and frequently counterproductive. As a result, there is greater emphasis on the importance of education, training, and establishing social norms against abuse of resources.

The role of the U.S. federal government is increasingly noticeable throughout the literature, in research undertaken by federally funded bodies as well as in an increased desire by Congress to have the bureaucracy take a greater role in preventing incidents and

mitigating damage they cause.⁵ Federal computer-related statutes, including the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA), reinforce the importance of data in the minds of our workshop participants.

Our findings from the workshops center around three areas: the importance of individual roles in incident perception, the variables used in deciding the seriousness of an incident, and what participants believed were the most significant factors in causing incidents.

Models, Roles, and Perception of Incident Severity

In one experiment, we asked participants to sort 21 incidents based on focus—people, data, or systems—according to the ICAMP-II model. In categorizing incidents by their focus, participants agreed on the primary focus of the incidents and were consistent in controlling for role and incident severity. These findings support our hypothesis that a common categorization model and incident language are possible and practical.

Role did seem to be a significant factor in determining how serious various incidents were perceived to be. Workshop participants seemed to have a set of variables in mind—based largely on the individual’s role—as to what makes an incident serious and what the next appropriate steps should be for handling it. Moreover, role seemed to influence which incidents were perceived as most serious. This is an important finding because setting incident-handling priorities requires that individuals within an institution agree on which incidents are most serious. Without such agreement, resources may not be deployed in the optimal fashion.

The effect that role plays on incident perception may be connected to the observed increased delineation of specific responsibilities within campus IT organizations. This might itself be an artifact of the increasing need for specialization, especially within rapid-reaction incident handling.

Variables Determining Incident Seriousness

What variables determine how serious an incident is deemed to be? Are there thresholds—either of incident type or potential impact—that trigger action? We sought to answer these questions in two ways. First, participants were given six long incident descriptions for which they were asked to rate the incident on its seriousness and explain in their own words the reasons that they came to their conclusion. Second, participants were given a list of ten variables and asked to select the five they deemed most important in judging incident severity. The results were then collated, and the top four variables from participant responses were paired against one another. Participants then picked what they deemed the more important variable from each pair.

We analyzed responses from the first experiment and found that one variable—risk of harm to people—stood out as the most frequently given factor affecting perceived severity, cited more frequently than the next two variables combined. The next two—potential criminality in an incident, and the perception that the incident is “not my job” or responsibility—were reported only slightly more frequently than five other variables. In all, the six most frequently cited variables in determining incident severity accounted for more than half of all participant-volunteered answers.

The second experiment allowed us to use more scientific means of analysis. By using matched variable pairs, we ascertained the relative importance of variables against one another. We found that “probability of danger to person(s)” was by far the most commonly selected variable, followed by “type and sensitivity of data involved” and “probability of further access/damage.” It is noteworthy that the most commonly selected variable in the matched pairs was also the most frequently volunteered in the free-response exercise. This is likely an artifact of our incident models, two of which featured or implied imminent danger to people.

Perceived Incident Causes

In the final part of our workshops, we asked participants to view brief descriptions of incidents and brainstorm the factors that could have made the incidents possible—what we call causative factors. We then analyzed the factors that were identified for commonalities and agreements. “User education (or lack thereof)” was the most frequently identified causative factor for the incidents reviewed. This was followed by “poor or nonexistent policy,” “too much or inappropriate access,” and “lack of physical security.”

Although we cannot draw hard conclusions from this exercise, it is clear that adequate user education and the existence of good policy are important factors in the minds of our respondents with respect to the prevention of future incidents. Further research into the factors that cause incidents is the primary focus of the second phase of our research, the CIFAC-NSF study.

Impact on IT Security Professionals

Our results carry significant implications for IT professionals. First, we see both a desire for and the possibility of a common language, complete with incident models, for discussing the origins of incidents, what they do, and how to prevent and mitigate them. This is a language that can transcend technical staff and be employed by higher education administrators and others with an interest in keeping computers and users happy and healthy.

Second, having a common language allows university officials to take a risk-management approach to IT security, leading to more coordinated efforts of security professionals and administrators to prevent and manage incidents. Risk management allows for optimal deployment of security resources and helps keep the accountants satisfied, which can mean more resources. In addition, a common language allows for codified rules of action, resulting in less second-guessing based on hindsight.

More information about the impact of this research on IT professionals can be found in a presentation made at the

2004 EDUCAUSE Security Professionals Conference, available at <<http://www.educause.edu/LibraryDetailPage/666&ID=SPC0412>>.


Conclusion

While the primary purpose of the CIFAC-EDUCAUSE project was to lay the groundwork for the larger CIFAC-NSF project, we learned valuable lessons about the way in which incidents are perceived and the current state of practice in incident prevention and management. Most significantly, our research seems to show a change in practice and belief in the past few years. Incident handling is increasingly specialized, as evinced by the “not my job” responses many respondents gave to incidents outside their area of expertise and by the undefining of events that were considered incidents just five years ago. At the same time, participants indicated an increasingly interdisciplinary method of management, with nontechnical personnel, including student-affairs staff and university counsel, playing an important role in incident management.

We should note, however, that without a common language for discussing incidents, it is impossible to achieve a universal definition of incidents and a full understanding of the institutional risk that computer-related incidents bring. Workshop participants indicated that the growth of a common language would be beneficial to them and their colleagues, a motif repeated frequently in the academic and practical literature.

Finally, we see overall a much more people-centric view of incident management than existed just five years ago. The emphasis that incident handlers place on user education indicates a widespread acceptance that technological fixes are not always ideal or even possible; the importance of danger to person(s) in evaluating incident seriousness is likewise encouraging. As information systems have become the lifeblood of campuses, the people they touch and the data they maintain are seen as requiring vigilant protection.

We welcome comments regarding our research, including those from

colleges, universities, and corporations interested in participation in the CIFAC-NSF study. Send comments to <cifac.staff@umich.edu>. 

Endnotes

1. The project aims to build on previous work by the principal investigator, Virginia Rezmierski, undertaken in the Incident Cost Analysis and Modeling Projects (ICAMP) <<http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml>> and the Logging and Monitoring Project (LAMP) <<http://www.aacrao.org/publications/catalog/NSF-LAMP.pdf>> (both URLs accessed September 9, 2004).
2. For the purposes of our study, we consider an incident to be any action/event that takes place through, on, or involving IT 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 or target individuals, systems or networks, or data resources and result in a policy, education, disciplinary, or technical action. See our report to EDUCAUSE, <<http://www.educause.edu/ir/library/pdf/SEC0409.pdf>>, pp. 9D15, for more about definitions.
3. See <<http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMPReport2.pdf>> for the model and full report (accessed September 9, 2004).
4. More detailed information on our workshop procedures and methodology is available in our report to EDUCAUSE, <<http://www.educause.edu/ir/library/pdf/SEC0409.pdf>> (accessed September 9, 2004).
5. In particular, the National Institute of Standards and Technology has published several valuable (and in our opinion under-cited) research studies, available at <<http://csrc.nist.gov/publications/nistpubs/>> (accessed September 9, 2004).

Daniel Rothschild (drothsch@umich.edu) is a graduate student at the Gerald R. Ford School of Public Policy at the University of Michigan. Virginia Rezmierski (ver@umich.edu) is an adjunct associate professor at the Gerald R. Ford School of Public Policy and the School of Information at the University of Michigan. She is retired as the Director of the Office of Policy Development and Education at Michigan.