FINAL REPORT OF THE
COMPUTER INCIDENT FACTOR ANALYSIS
AND CATEGORIZATION (CIFAC) PROJECT

VOLUME I: COLLEGE AND UNIVERSITY SAMPLE

Virginia E. Rezmierski, Ph.D.
Daniel M. Rothschild, M.A., M.P.P.
Anamaria S. Kazanis, M.A.
Rick D. Rivas, M.P.P.

This work was made possible through funding from the National Science Foundation and the EDUCAUSE-Internet 2 Security Task Force. The results and opinions expressed in this report are those of the researchers and should not be construed to represent the views of the National Science Foundation, EDUCAUSE, Internet 2, or the University of Michigan.
Table of Contents

Executive Summary 3

Acknowledgements 5

I. Introduction and Background 6
II. Pre-Study Concept Exploration 10
III. Study Preparation 13
IV. Data Collection and Management 19
V. Analyses and Findings 22
VI. Summary of Findings 38
VII. Conclusions and Recommendations 42
VIII. Reflections and Next Steps 49

Appendices
   A: Literature Reviews 52
   B: CIFAC Instrument 63
   C: Participating Colleges and Universities 71
   D: Sample of CIFAC Incidents 72
   E: Statistical Analysis 74
   F: Best Practice Scoring Scales 83
   G: Rationales For Ratings by CIOs 86

© 2005 the Regents of the University of Michigan. All Rights Reserved.
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.
Executive Summary

An extensive review of existing literature and feedback from the field led researchers to conclude that confusion exists within higher education in the management of computer-related incidents due to overly restrictive definitions of incidents, too technical a focus on prevention, and the expectation of malicious intent as the primary cause of incidents. A clear and robust framework was felt to be needed through which incidents could be viewed and the best management strategies elucidated. The need for metrics to guide decision-making within institutions was also noted. Finally, the literature and feedback convinced researchers that a broader institutional focus was needed in the identification and management of computer-related incidents: a focus that lifted what is currently a burden placed primarily on computer system administrators and which brought the professional perspectives and skills of different administrative departments to bear in preventing, assessing, and managing computer-related incidents. To address these issues, the Computer Incident Factor Analysis and Categorization project was undertaken.

The Computer Incident Factor Analysis and Categorization, or CIFAC, project was designed to:
1. Ensure increased awareness and involvement of risk managers, auditors, executive management, security administrators, law enforcement officials, university counsel, and relevant professional organizations;
2. Develop trust relationships with key academic and corporate managers for effective sharing of computer-related incident data;
3. Develop a common language for discussing a fuller range of computer-related incidents; and
4. Isolate, define, and analyze the variables that are related to the occurrence of different types of incidents within these settings.

The CIFAC study utilized a direct contact, in-person data collection methodology, to collect data from a diverse sample of 36 colleges and universities. This resulted in enthusiastic participation of over 90 respondents and yielded data on 319 computer-related incidents. Approximately three retrospective incidents (those occurring within the past 12-18 months), and three current incident (incidents within the last three months of the data collection period) were collected from each respondent, resulting in a total of 250 retrospective and 69 current incidents in the sample.

A data collection instrument was used in direct interviews with participants to collect information about their perceptions of the importance of over 80 variables in causing each of the reported incidents. The interview survey also facilitated collection of information about prevention strategies for that incident and “best practice” recommendations for prevention, mitigation, and management of the incident. Researchers collected data regarding the perceived seriousness of each incident and the variables that caused respondents to rate one incident as more serious than another.

Analysis of data showed that a lack of sufficient training and education was identified as the most frequent cause of the incidents reported. Having policies in place, enforcing policies, and providing user awareness training was considered the most important factor in preventing the incidents from happening.

The strength of this finding is surprising and was made clear by descriptive statistics and factor analysis. The importance of training and education appeared yet again when researchers analyzed the best practices that were recommended by participants for prevention, mitigation, and management of incidents. The findings of this study are clear. Having policies in place, making people aware of the requirements and policies, reinforcing them through education and good procedures, and providing training and education were identified by CIFAC...
respondents as among the most important steps that could be taken to prevent the computer-related incidents that are occurring in colleges and universities. These are the places for IT resource expenditure on campuses.

Four factors appeared to be responsible for the majority of variance in participant responses. Of those four factors, three were people-related and one was network-related:

- For factors related to IT personnel, it appears that more education and training, improved job requirements, and procedures that help prevent them from making accidental or careless mistakes are important in preventing the incidents.

- For factors related to users, it appears that more education and awareness training, more stringent requirements, and better knowledge of policies and systems prior to the use of campus networks would be helpful in preventing them from accidental or careless behaviors, thereby preventing the incidents.

- For factors related to non-IT staff, more education, more stringent job requirements relative to technology use and data protection, and having more knowledge prior to using the computer systems would prevent accidental and careless behaviors that are one of the causes of incidents.

- For factors related to networks, more resources, more and better procedures and requirements relative to configuration of software and hardware would be helpful in preventing the incidents that are occurring.

Three stimuli to action were significantly related to the perceived seriousness of an incident: probability of damage to institutional reputation, number of people affected, and probability of damage to a person. When any of these items were present in an incident, it was considered more serious and action more necessary.

During this project the CIFAC research staff made a number of noteworthy observations.

- Many incidents with a wide range of targets and scope are happening in colleges and universities.
- Students are a major factor in these settings, but may not be the primary factor in the biggest technology-related risks to the campuses.
- IT staff members need to talk about and be supported in handling incidents.
- There is an increase in the use of technical incident prevention measures on campuses.
- Interdepartmental incident response teams are increasingly being used for incident response.
- Having policies, procedures, and practices in place prior to incidents occurring is very important to mitigating their overall costs.
- Extensive education and training for both IT staff and users is very important.
- The use of automated response and enforcement tools is important.
- Risk managers and auditors seem to be largely absent from the interdepartmental incident handling teams, to the detriment of overall enterprise risk awareness and management.

The report provides more detailed findings, conclusions and recommendations. The authors also discuss five major needs that seem to explain the strong findings of this research: policies and procedures, training and education for IT staff, training and education for users, increased security awareness campus-wide, and additional control mechanisms that allow quarantine zones and more stringent detection and management of incidents.
Acknowledgements

The staff of the CIFAC project acknowledges the considerable contributions made by organizations and individuals in support of this project.

We especially acknowledge and thank the Chief Information Officers and information technology staff members from the thirty-six colleges and universities across the United States who gave willingly of their time and expertise in providing information and insights regarding computer-related incidents. They altered their busy schedules to arrange meetings with members of the research team, engaged enthusiastically in the data exchanges, and showed high levels of professionalism as they worked with us to try to identify best practices for preventing and managing the computer-related incidents that are occurring.

We acknowledge and thank the Division of Information and Intelligent Systems within the National Science Foundation for their support and funding of this project. The enthusiastic and interested responses that we have received from the unit chief, Dr. Suzanne Iacono, from early formation of our idea for this project through to analysis of data and conclusions, has been very much appreciated.

We acknowledge and thank EDUCAUSE, Inc. and the EDUCAUSE-Internet 2 Security Task Force for their support and early funding of our exploratory activities and preliminary research efforts. Of particular attention in this regard was the support provided by Dr. Rodney Petersen for helping us to attract participants to our focus groups and for his assistance in conceptualizing the role of these groups and analyzing their responses.

We speak more about the importance of the CIFAC Advisory Board later in the report, but here too, we wish to acknowledge and thank the members for their willingness to serve as our advisors, for their participation in phone conference calls, their travel across the country for board meetings, and their time in reading progress reports and editing this final report. Most importantly, we thank them for their continued support and encouragement as this project was refined, implemented, and the data analyzed and interpreted. Their ideas and trust were critical to the success of this work.

Our gratitude goes also to staff and administrators of the University of Michigan-Ann Arbor, who helped us develop and pilot our instrument and who supported our research administratively through-out the project. The support and careful attention to detail provided by Ms. Lori Coleman was of particular importance to the financial management of this project. We also wish to offer heartfelt thanks to Ms. Jill Crane, Ms. Margie Cohen, and Ms. Sharon Disney for their administrative support and help with travel and logistics. Additionally, Mr. Brady West of the University of Michigan’s Center for Statistical Consultation and Research gave generously of his time and expertise in helping us review our statistical results and express them in a manner that was accessible to non-specialists; any confusion that the non-statistician might find in our results remains wholly the fault of the project staff.

Without the support, encouragement, and shared insights of the people and groups mentioned above, and without the tireless work, shared expertise, and energetic debates of the CIFAC research staff, this project would not have been accomplished. We are very grateful for the synergy that was formed.
I. Introduction and Background

A. Introduction

This report – Volume I of the Computer Factor Analysis and Categorization Project Final Report – will focus on data collection and analysis accomplished on a large college and university sample. In May 2005, a supplemental grant was awarded to CIFAC to expand the study to include a small corporate sample. Upon completion of the data collection and analysis from the corporate sample, an addendum – Volume II – will be submitted to NSF to complete the full reporting for the CIFAC project.

In this volume, we will discuss the pre-study conceptual explorations that were undertaken with funding from the EDUCAUSE-Internet 2 Security Task Force, the study preparation, data collection and methodology, the analyses, findings, conclusions and recommendations. This report will also provide the author’s brief reflections on next steps to be taken and the dissemination of results. Appendices attached to this report will provide useful detail for those wishing to go deeper into the project’s processes and findings.

B. Background

Prior to beginning this project, researchers heard a call from the field for a common language – a widely agreed upon terminology for discussing and sharing information about computer-related incidents. We undertook an extensive review of the literature to better understand the issues surrounding terminology in this field. The review was completed with financial support from the EDUCAUSE-Internet 2 Security Task Force; it has been reproduced in Appendix A of this report.

From that literature review, three important conclusions will be discussed here to provide background for the CIFAC study – background that will help readers understand the focus of our efforts. In our report to the EDUCAUSE-Internet 2 Security Task Force, we emphasized the need for precision as professionals discuss and share information regarding computer-related incidents. We argued:

An imprecise or overly broad definition of an incident allows policy writers and response teams to slide into a postmodern morass where everything is simultaneously both an incident and not an incident.

The literature review allowed us to draw conclusions regarding the definition of incident, regarding taxonomies and categorizations, and regarding the need for metrics.

1. Conclusions Regarding Definitions

Our review of the literature led us to conclude that extensive confusion exists because of too restrictive definitions of incidents, too technical a focus, and the imposition of implied malicious intent. We recommended that a less security-oriented and technically focused definition of incidents should be supplanted by a broader and more organizational risk-focused definition; we implied that the conceptualization of incidents needed to shift from a micro to a macro perspective. We concluded that the scope of threat to the college or university as a whole, as well as the institutional mission, must be recognized and carefully considered as “computer-related incident” is defined. Any such definition must also include risks to electronically-stored data, including corruption, falsification, theft, and improper dissemination; such a definition must transcend technical security measures and be cognizant of the damage that non-security incidents can cause.


2 Ibid.
Our primary obligation in this attempt to define computer-related incidents is to institutions of higher education. Our conclusion is that efforts which narrowly define incidents as security-related such as in the aforementioned definitional literature authored by FedCIRC and TERENA are too restricting and can leave responders unnecessarily myopic as they search for best practices and the most effective responses to computer-related incidents. We, like Grance et al. (2004), recommend that each college and university clarify its terminology prior to managing incidents and set specific tolerance and response thresholds for particular types of incidents. Still, a common set of basic terms must be adopted across colleges and universities if we are to learn from each other.

The CIFAC researchers recommended the following definition. It is indebted to the work of Grance et al. (2004, p. 2-1.), who write that “an incident can be thought of as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” Our work incorporated our own experience, comments from professionals in workshops and personal interviews, and commentary from the literature reviewed in this report.

“Computer-related incident” is defined for the purposes of the CIFAC study as “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.”

2. Conclusions Regarding Taxonomies and Categorizations

The concepts of “taxonomy” and “categorization” are, despite their frequent use as synonyms, inherently different ideas. They differ in terms of type of organization and the narrowness of their focus; in practice, in whether they focus entirely on technical vulnerabilities, or on the larger realms of incidents and security events. This distinction was particularly relevant to the CIFAC study, as we sought to look at the full range of computer-related incidents.

We believed that there is a fundamental difference between the lists of system vulnerabilities or individual incidents that have appeared in the literature and a common language or a typology for describing and classifying or categorizing the fuller range of computer-related incidents. The categorization system we sought was one that helped administrators to understand incidents that target individuals, those that target systems (about which much has been written), and also incidents that target data and/or intellectual property. Managers of information systems, and certainly the executive officers of an organization, must be aware of all three categories of incidents and the risks each type brings to the IT group and the college or university. Therefore, we must better understand the different types, and the factors leading to the occurrence of each, to improve the security of our systems and our responses to the incidents once they occur.

The need for a clear and robust framework through which to view incidents, their causes, and their management is evinced by the literature and discussions in the CIFAC/EDUCAUSE focus groups. Academics and practitioners have been working on creating such a framework for over a decade, primarily by suggesting taxonomies, lists, and categorizations. Each method has its own strengths and shortcomings.

Taxonomies create clear and logical structures, but they often prove too unwieldy and compartmentalizing for practical application. That no characteristic of an IT incident is inherently a priori any other further mitigates the appropriateness of a taxonomical view of incidents. Lists provide comprehensive coverage of known vulnerabilities, but they do not illustrate any causal, contributory, or prescriptive associations between these vulnerabilities; moreover, they tend to be specific to an operating system, program, hardware configuration, or protocol and therefore do not posses the universality that should be a salient characteristic of any inter-organizational incident discussion framework.

Categorization schemes exist somewhere between taxonomies and lists; they serve to give some order and universality to lists without creating too rigid a system of hierarchies. The beauty of categorization schemes is that they are simultaneously ductile and rigid; they allow institutional modification and adaptation without sacrificing the minimum level of stringency to make them useful across institutions and fields. Categorizations provide guidance for incident handling and management, offer simplicity for easy application, and allow data sharing for analysis purposes without excessively cordoning off incidents based on a particular, and essentially arbitrarily chosen, characteristic. For these reasons, we believe that a categorization system will provide the most value to both technical and non-technical practitioners of incident prevention and management.

The CIFAC study therefore used a three part categorization scheme: incidents focused on people, incidents focused on systems, and incidents focused on data. We explored the utility of such a categorization system and the relationship of such incident types relative to seriousness and to the best practices recommended by our respondents.

3. Conclusions Regarding Need for Metrics

Our review of the literature showed that the need to recognize and encourage consideration of human motives, objectives, and the impact or results of the incident is being increasingly emphasized in current prescriptive literature. It brings the focus of computer-related incidents into more alignment with the work of risk managers and auditors as they seek to protect colleges and universities from risks. There is an irony in that ten years ago, Neumann was writing about such computer-related incidents and calling his work *Computer Related Risks*. Now, we are again focusing on the relationship of computer-related incidents and organizational risks. This maturing perspective on incident management is more inclusive, wider, and requires the involvement of others to ensure sufficient organizational perspective and the exercise of best practices.

Other literature, including that of a more technical bent, shows this shift to a more risk management approach and toward the use of metrics in viewing and responding to computer-related incidents. Like Austin and Darby, we realize that companies need to have smart technicians who use lists and taxonomies of vulnerabilities, stay abreast of technical research in their field, and quickly obtain information, upgrades, and patches from vendors and the free and open source software (FOSS) community to secure their systems. But the opinion that they should not “be calling the shots” on incident management and response, to quote Austin and Darby, seems to be gaining prominence within colleges and universities and the literature addressing these institutions.

We concluded that systems administrators should not be inappropriately burdened with the role of determining the priority rating that different types of incidents receive on a criticality or seriousness scale, or setting the thresholds for when certain types of incidents get escalated to include others in the incident management and decision-making process. While, in the past, the systems and network staff have been alone in understanding how computer-related incidents were happening, we cannot continue to ask them to carry the burden of these decisions as well as perform the technical duties that are required. Experience and a better understanding of the nature of computer-related incidents has led to a more comprehensive and wider view of incident management, one that does not rely on lists or taxonomies or technicians, but that calls for other tools to assist in this more risk management approach. This new approach involves codification/categorization, defining thresholds for response, and responding through proven best practices.

C. CIFAC Objectives

The CIFAC project accomplished the following four objectives:

---

1. Design a project support and participation structure that ensures increased interdisciplinary awareness and involvement of risk managers, auditors, executive management, security administrators, and relevant professional organizations.

2. Develop trust relationships with key managers within academic and corporate settings for effective sharing of computer-related incident data.

3. Develop a common language for discussing computer-related incidents, a language that encompasses the fuller range of incidents and allows for the classification of incidents in a reliable and understandable manner.

4. Isolate, define, and analyze the variables that are related to the occurrence of different types of incidents within these settings.

The project was designed to:

- Increase awareness of security and computer-related incidents among members of different disciplines,
- Create the vehicle for high-level discussion of issues and sharing of ideas,
- Instill an investment in the final product within participants in the project, and
- Establish a willingness to, and mechanism for, disseminating the results of the project to the field.

The project began to meet its objectives through a series of pre-study focus groups supported by funding from the EDUCAUSE-Internet 2 Security Task Force and through very careful study preparation. Both will be discussed next in this report.
II. Pre-Study Concept Exploration

A. EDUCAUSE-Internet 2 Security Task Force Focus Groups

In preparation for CIFAC Objectives 1 and 3 above, and with funding from the world’s largest professional higher education technology and policy organization, EDUCAUSE, researchers began a series of conceptual explorations. We wanted to test ideas having to do with the categorization of incidents and to learn more about how professionals responded to the perceived seriousness of incidents.

In our initial meetings with security and technology professionals on the University of Michigan-Ann Arbor campus, we were told that computer-related incidents have not significantly changed over the past three years, since our previous research was completed. We learned however, that while the nature of incidents seemed not to have changed, current incidents are perceived to be larger in magnitude, focused more on systems and networks, and that perpetrators and intrusion detection and prevention mechanisms are perceived to have grown increasingly sophisticated over the last three years.

Three professional focus groups were organized to continue these conceptual explorations. One-day workshops were held at Indiana University’s campus in Bloomington, Indiana; at the Big Ten Conference Center in Chicago, Illinois; and at Carnegie Mellon University’s CSIRT office in Arlington, Virginia. A total of 33 individuals from 24 colleges and universities provided data to our preliminary study. Participants were selected based on their experience with computer-related incidents on college and university campuses with an eye to inviting people from diverse areas of incident management.

A series of small exercises were undertaken in the three focus groups. They will be briefly described here to show how basic concepts developed for the CIFAC study.6

1. Focus Group Exercise #1

The first exercise was simply designed to identify participants’ primary roles within their institutions and to describe the respondent sample. Participants included system administrators, network security manages, policy directors, data managers, database administrators, security officers, chief information officers, compliance officers, user support personnel, and a college associate vice president. Researchers found these focus groups and the responses of our participants to be very helpful in introducing concepts that should be further studied in the second phase of the CIFAC Project.

2. Focus Group Exercise #2

Participants were given descriptions of six fictionalized incidents which the CIFAC staff had based on actual historical incidents. Each incident description was approximately 150-250 words in length. For each incident, participants were asked to:

1. rate the seriousness of the incident on a scale of one to four (low seriousness to high seriousness) with respect to the urgency for response, and
2. identify the variables or statements within the incident that they considered important in evaluating its seriousness with respect to the urgency for response.

This exercise was designed to answer a number of questions that were critical to the organization of the second phase of the project. How serious was each incident perceived to be from the perspective of these participants?

6 Greater detail about these processes can be found in the CIFAC report to EDUCAUSE (see footnote 1 for citation and URL).
Were there significant differences in seriousness ratings between incidents? What correlations existed between the existence of a variable in an incident and that incident’s seriousness ratings? And were there differences in the variables identified by each of the groups of participants?

We found that the seriousness ratings were very similar for four of the six incidents. Two of the incidents had significantly different seriousness ratings than the other four incidents. We sought to determine which variables within these incidents were associated with differing perceptions of seriousness amongst our participants.

A content analysis of the six incidents was completed to learn more about the variables within these incidents. We found that primarily three variables within the incidents explained the difference in ratings: quantity or extent of loss, importance or level of people involved, and the potential of further damage, access, or danger.

To understand priorities in perceived seriousness we tabulated written responses from each of the incidents, assigned a name to the variable or phrase and analyzed the results. We found that “probability of danger to people” was the variable most associated with a high perceived seriousness of an incident.

In the larger CIFAC-NSF study, we partially repeated this exercise by asking each of the CIOs from the 36 participating colleges and universities to rate four of the incidents used in the focus groups in terms of seriousness and to identify the factors within those incidents that they felt were important to determining their ratings. The results of the CIO ratings, and these results from the preliminary focus groups, will be discussed in more detail in the Analysis and Findings section of this report.

3. Focus Group Exercise #3

Participants were given a list of 10 variables that might be used to judge the severity an incident and were asked to indicate the five most significant to them in making their judgments of seriousness when facing an incident. The researchers selected variables for this list from the literature, from previous research, and from consultation with relevant professionals. The responses were tabulated and the four highest scoring variables for the focus group were paired against each other. A forced choice was then required: respondents were asked to select within each pairing the most important variable in evaluating severity of an incident.

A score for each variable was calculated based on the aggregate number of times that it was seen as being more important than the variable it was paired against. The highest theoretical score for any variable was 99, which would indicate that every respondent selected that variable when paired against every other variable. We found that “probability of danger to person(s)” was consistently seen as most important variable in making decisions about the seriousness of an incident.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Cumulative Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of danger to person(s)</td>
<td>83</td>
</tr>
<tr>
<td>Type and sensitivity of data involved</td>
<td>50</td>
</tr>
<tr>
<td>Probability of further access/damage</td>
<td>37</td>
</tr>
<tr>
<td>Cost to the department/college/university</td>
<td>15</td>
</tr>
</tbody>
</table>

4. Focus Group Exercise #4

In exercise #4, participants were each given a stack of 21 cards on which brief descriptions of standard incidents were written and a seriousness rating scale of one through four was provided. Participants were asked to rate the seriousness of each of the incidents, and then once rated, to distribute each card into a bin designating the focus of the incident as relating to people, data, or systems.

In this exercise we sought to determine if people in different roles can agree on the primary focus of a computer-related incident, what the perceived seriousness level of incidents in each of the categories might be, and if there is agreement on the seriousness of incidents in each category.
We found that all three groups of participants could reliably agree on the sorting of the 21 incidents by the focus of the incident.

<table>
<thead>
<tr>
<th>Target</th>
<th>Frequency</th>
<th>% of incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems/networks</td>
<td>253</td>
<td>36.6%</td>
</tr>
<tr>
<td>Data</td>
<td>151</td>
<td>21.8%</td>
</tr>
<tr>
<td>People</td>
<td>288</td>
<td>41.6%</td>
</tr>
</tbody>
</table>

Table 2

We learned that participants in different roles, with limited amounts of information about a particular incident could sort the incidents by the focus of the behavior into the three categories, of people, systems/networks, and data with statistically significant agreement among respondents.

We also learned that participants could identify the factors that appear to be related to the occurrence of an incident. However and perhaps more importantly, participants have some agreement as to the variables that make an incident serious and agreement on the categorization of the incidents by focus.

5. Focus Group Exercise #5

In the previous exercise, participants were asked to read brief incident descriptions presented on a screen and identify the factors that made each incident possible. The research team then analyzed the factors that were identified for commonalities and agreements.

Analysis of the responses revealed 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.” “Too much or inappropriate access” and “lack of physical security” also occurred more frequently than all of the other identified factors, perhaps also reflecting poor or non-existent institutional policy or insufficient user education. However, there is insufficient information from this brief exercise to fully understand what information in the incidents or from respondents’ personal experience caused them to volunteer their particular answers. We were able to conclude however, that adequate user education and the existence of good policy are important factors in preventing incidents in the minds of our respondents.

The CIFAC-EDUCAUSE effort highlighted several potentially important analyses to be pursued in the CIFAC-NSF project, especially the investigation, delineation, and evaluation of factors and their relationship to incident occurrence.
III. Study Preparation

In preparing for the larger CIFAC study, three elements in the project design were particularly important: the establishment of a high-level advisory board, the design of a careful and personal approach in identifying and interacting with the participant pool, and the design and development of a data collection instrument. They are briefly discussed in the following sections of this report.

A. CIFAC Advisory Board

The CIFAC Advisory Board was created to accomplish, among others, Project Objective 1 (increased interdisciplinary awareness and involvement of risk managers, auditors, executive management, security administrators, and national professional organizations.)

The Board is composed of the following individuals:

- Shawn A. Butler  Associate Professor of the Practice, Carnegie Mellon University
- Mark S. Bruhn  Chief IT Security and Policy Officer, Indiana University
- Robert N. Clark, Jr.  Director of Internal Audit, Georgia Institute of Technology
- E. Eugene Schultz  Senior Engineer, Lawrence Berkeley National Laboratory
- Barbara Simons  IBM Research Staff Member (retired) and Past President, Association for Computing Machinery (ACM)
- Eugene H. Spafford  Professor and Executive Director, Center for Education & Research in Information Assurance and Security (CERIAS), Purdue University
- John J. Suess  Vice President for Information Technology, University of Maryland- Baltimore County
- D. Frank Vinik  Senior Risk Analyst, United Educators Insurance
- Rodney Petersen  Project Coordinator, Security Task Force, EDUCAUSE
- Tracy Mitrano  Director of Computer Law and Policy and Adjunct Assistant Professor, Cornell University

The diversity represented by members of this Board has helped to accomplish a portion of Objective One. Members of the Advisory Board have assisted in recruiting participants for the subject pool. They have also assisted in disseminating preliminary information about the project and about information security issues nationally. Five members of the Advisory Board and the project principal investigator are among those quoted in a recent article in the Chronicle of Higher Education entitled “Insecure and Unaware: An analysis of campus networks reveals gaps in security.”7

This interdisciplinary board benefits the project by providing support and insight to the project team. The different perspectives and rich interdisciplinary mix benefit the research because the members continue to provide important insights and suggestions for analysis and interpretation of results. It benefits the members as well in that several have commented on how much their own awareness of issues and concepts has been expanded through participation with the CIFAC project. And finally, it benefits the field through active dissemination of results and knowledge. As one of the members recently commented:

I am learning a lot from your research and think that it is incredibly important. Top people in my organization are starting to become very interested in this issue given the rash of highly publicized recent incidents in higher education. We are trying to figure out best risk management practices in this area, and the work of CIFAC will be of invaluable assistance. I know that research can be very tiring.


13
work, but I think you and your team are making a major contribution in an area that has been under-studied in the past.\(^8\)

Every member of the CIFAC Advisory Board has agreed to continue serving as a CIFAC Advisory Board member while the project extends its work into 2006 to collect and analyze the corporate sample.

### B. Preparation of the Participant Pool

Preparation of the participant pool involved identifying and selecting participants for the sample and building trust relationships within the various institutions.

#### 1. Sample Selection: Geographic Location

To minimize travel costs, maximize the efficiency of data collection, and manage within the budget of the CIFAC project, colleges and universities within six geographic areas were targeted for potential project participation. The sample is not random; that is, we did not take the full list of potential colleges and universities and randomly select those to participate. Rather, we identified a west coast, northeast, south central, southeast, Midwest, and Michigan cluster of schools. Within those geographical areas, we selected schools to represent a mix of public and private institutions with diversity in enrollment size – large and small/medium schools. Large schools were defined as those with a full-time equivalent enrollment of 10,000 or more students, while small/medium schools were those with less than 10,000 full-time equivalent students. Both graduate and undergraduate students were used in this calculation.

#### 2. Sample Selection: Institutional Type and Size

Because there is a strong correlation between public status and large enrollments, we knew that special attention would have to be paid to the upper right and lower left quadrants of our sample selection matrix.

Information about the size of the school student populations was obtained from the EDUCAUSE web site in the membership directory which reflected 2001 Department of Education data. The resulting distribution was as follows:

---

\(^8\) Vinik, F. (2005, June 15). Personal email to principal investigator.
We noted that, while each cell was not equal, the private-public and large-small/medium column and row totals were thus roughly equivalent, meaning that the criteria of interest were sufficiently well represented and meaningful.

<table>
<thead>
<tr>
<th></th>
<th>Public</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large</td>
<td>11</td>
<td>9</td>
</tr>
<tr>
<td>Small/Medium</td>
<td>6</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 3

3. Sample Selection: State Data Protection Legislation

One final variable was considered in the selection of our sample. We were interested to know if the prevalence or absence of state data protection legislation had an effect on the data provided by participants in those states. We used data collected by the Electronic Privacy Information Center (EPIC) on the existence of laws relating to data protection in twenty categories for all 50 states plus the District of Columbia to give each state a “data protection score” based on the quantity of data protection laws. A state with laws in twelve of the twenty areas identified by EPIC, for instance, would be given a score of twelve. While we did not use information about the prevalence or absence of state data protection legislation to determine the sample for the study, we did review our sample to ensure that in our later analysis we would be able to control for the prevalence of state regulation in examining, for instance, the perceived seriousness of data-related incidents.

4. Building Trust Relationships

The CIFAC proposal discussed, at some length, the difficulty in collecting computer security data and specifically information about computer-related incidents. It also stressed the importance of “trust relationships.” Project Objective 2 states: “develop ‘trust relationships’ with key managers within academic and corporate settings for effective sharing of computer-related incident data.”

In the CIFAC NSF grant proposal, referring to the difference in privacy expectations between college and corporate populations, the PI wrote:

This dynamic (lack of trust) may create a sense of tension therefore between researchers from academia doing research within academic and corporate environments. For this reason, the establishment of trust and credibility with specific individuals within a participating organization is very important. Indeed, it may be critical to the researcher’s ability to obtain needed data regarding categories and occurrence-related factors.

The PI emphasized the importance of the direct contact methodology, a feature of the research which increases the personnel and travel costs but also enhances the effectiveness of the data collection. Rezmierski wrote:

While this method is people and time intensive, as reflected in the budget, experience has shown that the best data are collected using this model. The outcome of such careful nurturance of study participants is that partnerships are formed, organizations become more accessible for the eventual

---

implementation of research tools, and data regarding this important research area become available for analysis.

Personal contact with respondents and a high-level authorization for data collection were considered very important to the CIFAC research team. Given the sensitive nature of the data being collected, it was important to ensure that the right participants were contacted, that they were authorized to speak freely with the research team, and that they were assured of data confidentiality within the CIFAC project.

The CIFAC team spent many months during the project’s first year identifying the appropriate project participants within participating institutions and establishing the trust relationships. Trust relationships and agreements to participate were established with 36 colleges and universities. In fact, 95% of the schools that were invited to participate enthusiastically agreed.

While there was obvious interest in the study, and an eagerness to see the results, identifying the appropriate people within each organization to participate and gaining the involvement of CIOs and their authorization for data collection was critical. At each of the selected colleges and universities, the chief Information Officer (or a similar such officer), was personally contacted and told about the CIFAC project. The CIOs were informed of obligations associated with participation in the project and were asked to identify up to three people within their organization to serve as participants in the study. Specifically, CIOs were asked to identify “the person who knows the most about, or handles computer-related incidents that are people-focused, the person handling systems-focused incidents, and the person for data-focused incidents.” As will be discussed later, these selected participants were expected to be professionals who were well-versed in the problems causing these incidents, the handling of the incidents, and were expected to be capable of providing detailed data and best practices relative to the incidents.

The CIOs of participating schools were asked to personally inform selected staff members that they were authorized to meet with the CIFAC research team and to provide data regarding three incidents that occurred within the previous 12-18 months and later to provide data regarding three additional incidents over the months following the campus visit.

From this point, the research staff had direct contact with each of the identified staff members for scheduling and data collection. Data collection for “retrospective incidents” (those occurring in the past 12-18 months,) was conducted by members of the research team in-person on each campus between September and December 2004. Additional incidents that were considered “current” were discussed and data were collected later via telephone until mid-March 2005.

5. Corporate Sample

Whereas the original project proposal called for 36 college/university and 18 corporate participants, due to NSF requested budget reductions at the time of the award, it was necessary to cut the sample size to 18 colleges and universities and nine corporate participants. A supplemental funding request was submitted to NSF in February to reestablish the project’s sample to its original size and thereby strengthen potential statistical analysis and increase the value of the project to the field. Since an NSF response to the supplemental request was delayed, and engaging corporations for data collection proved far more difficult and costly than anticipated, in April 2004 the research team decided to halt efforts to recruit corporate participants for the project and to move forward to expand and reestablish the pool of college and university participants to 36.
In May, 2005, NSF granted the supplemental funding for the CIFAC project. Therefore, the project will be extended for one year to 2006. The corporate sample will be identified and invited to participate. Data will be collected, analyzed, and compared, wherever possible with the college and university data. Volume II of this report will be submitted to NSF in 2006 discussing the results of this added sample population and the total sample at that time.

C. Development of Data Collection Instrument

1. Concepts and Definitions

Drawing upon the insights gained from our pre-study focus groups, the literature, and discussions with computer incident professionals, we developed an instrument that would attempt to collect information about incidents including type, perceived seriousness, factors that could have prevented the incident, factors that caused the incident, and factors that affected the speed and manner of reaction to an incident. The instrument was focused almost entirely on the incident being reported, not on the personal characteristics of the respondent. No personal information was requested of the participant or information about their employment histories or specific work responsibilities.

A commonly employed opinion category quantifier of four possible responses was created for and used throughout the instrument. The foils for the scale were “not at all,” “somewhat,” “quite,” or “extremely,” which preceded questions about importance of particular factors. Significantly, the scale provided no middle category, thus requiring respondents to tip each scale in one direction or the other.

Incident Definition
This definition of incident was provided at the beginning of our initial data collection meeting with each respondent:

A computer incident is defined as any action or 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 or target individuals, systems, or data resources and result in a policy, education, disciplinary, or technical action.

Concepts of Cause and Prevention
The primary inquiry in the CIFAC instrument was conducted through a set of prevention and cause questions. The research team struggled with the concepts of cause and prevention. In the beginning we sought information about causative factors, thinking that respondents would be able to say what had caused the incidents on which they were reporting. We also thought that certain facilitative factors might be identified, those conditions, while not directly causative, might have encouraged or allowed an incident to occur. As the instrument was piloted and discussed, it became clear that the incidents are often so complex that it is difficult for respondents to identify particular root causative or facilitative factors. The research team therefore decided to include a set of questions asking respondents to say how important they thought different items were in causing each incident. A somewhat parallel set of questions was included to identify how important respondents thought various items would have been in preventing the incident from occurring.

Concepts of Best Practices
A second set of important questions in the instrument focused on best practices. A set of questions, included for each reported incident, asked respondents to identify what they would recommend to a colleague as best practices for preventing the incident, mitigating the effects of the incident, and managing the incident. We expected best practices to be related to specific incidents. We knew that the term “best practice” connotes the most desirable among all possible practices. We also recognized that each of our respondents could not possibly know all potential practices for any given incident and that the volunteered responses were only the best practices as perceived by each respondent. We decided, however, to retain the terminology of “best practice” as an effective way to draw out thoughtful responses from participants and also hoping to gain insight into any patterns and practices that should be shared with the field, relative to particular types of incidents.
Concepts of Thresholds

One question asked respondents to identify how important each of a set of items was in causing them to act in response to the incident; we called these “stimulus to action.” In the focus groups that were held in preparation for the project, the notion of a “threshold” was introduced by the participants. This “threshold concept” seemed to imply a saturation point which created the need for action. The concept of certain factors, perhaps associated with different incidents, having differing weights or importance for signaling action, was interesting to the research team. Therefore we created a question in the instrument to explore the concept of a stimulus to action, in hopes of gaining more understanding of this notion of “thresholds” that was introduced by our participants.

General questions were also included in the instrument. A set of questions was included regarding the general demographics of the institution and its general incident handling practices. Two questions were included to draw information about how interdepartmental each school’s incident handling practices were by asking what institutional actors (e.g.: auditors, attorneys, student affairs staff) were included when an incident occurred. Another set of questions asked for their perception of the adequacy of their incident handling processes as they related to a particular incident.

2. Instrument Pilot Testing

The CIFAC data collection process relied on recalled information. Therefore, it was of the greatest importance to use a survey instrument targeted not only to the technical aspects of computer incidents, but that stimulated participants to recall the particular events surrounding reported incidents. To test the effectiveness of the instrument, researchers proceeded to conduct pilot tests.

After the first draft of the instrument was written, a pilot test was completed on the University of Michigan-Ann Arbor campus involving technical, non-technical, and administrative personnel. The test determined whether the instrument’s language was compatible with practitioners’ understanding of terms and whether the instrument effectively captured answers to the questions the research team was attempting to ask. Each of the three CIFAC staff members who would later be conducting field interviews and data collection participated in the pilots. Some interviews were conducted on a one-on-one basis, while others were conducted with a second CIFAC staff member present to observe the interaction between the interviewer and respondent.

After the first round of piloting, the researchers determined that some questions were perceived as ambiguous or that they did not effectively answer the questions we were attempting to ask. As a result, the questions were edited to be more specific and to use language that would be equally clear to persons from varying backgrounds and with differing institutional responsibilities. We reworked the questions in order to select words that implied a linear progression of severity on the four-point Likert scale.10

The second pilot test was conducted with five participants, some of whom had also participated previously. The revised instrument was found to be clearer and easier to use. It was determined that an average incident data collection session would take approximately 30 minutes.

The instrument was designed to be administered in-person and answers recorded using SPSS Data Entry 4.0 on a notebook computer, which allowed easy transfer to an aggregated data set. After the two rounds of pilot testing, the instrument was ready to be put into the Data Entry format. The final CIFAC data collection instrument appears as Appendix B of this report.

---

10 We are indebted to Brady West at the University of Michigan Center for Statistical Consultation and Research for his assistance with this task.
IV. Data Collection and Management

This section of the report provides information about the CIFAC study hypotheses, the data collection and management procedures, and the pooling of retrospective and current incident data.

A. Revised Study Hypotheses

During the development and piloting of the study instrument, it became clear that language used in the original study hypotheses, such as “causative and facilitative factor,” was too vague to be understood consistently by all respondents and that many incidents were too complex in nature to permit responses to such inquiries. Terminological and syntactic decisions were made during the development of the instrument. It was also decided that the corporate segment of the study would be delayed while waiting for supplemental funding. The original hypotheses included items regarding the corporate sample. Therefore, while the basic study foci did not change, the hypotheses were reworded to better reflect the language that was included in the data collection instrument. (See discussion of Development of Data Collection Instrument, above.)

Revised hypotheses are as follows. They use the terminology of “prevention and cause,” “stimulus to action,” and eliminated the corporate hypotheses for the time being.

1. In same-content questions, respondents will demonstrate a distinction between factors selected as important in prevention and cause.
2. There is no relationship between the rating of seriousness and the categorization type as assigned by our respondents.
3. There is no relationship between the rating of seriousness and each of the items on the stimulus to action question.
4. There is no relationship between the ratings of seriousness on a given incident and the rating of effectiveness of incident response.
5. There is no relationship between ratings of incident response and adequacy of pre-established procedures.
6. There is no relationship between ratings of incident response and degree to which procedures were followed.
7. There is no relationship between the category of incident and each of the items on threshold/stimulus to action.
8. There is no relationship between the items on threshold/stimulus to action and the type or size of the institution.
9. Across all of the incidents categorized as PEOPLE, a common set of factors exists.
10. Across all of the incidents categorized as DATA, a common set of factors exists.
11. Across all of the incidents categorized as SYSTEMS, a common set of factors exists.

B. Data Collection and Management Procedures

In early September 2004, CIFAC began its process of data collection from 36 colleges and universities. (A list of the 36 participating colleges and universities appears in Appendix C.) Up to three incidents were collected from up to three respondents at each of the 36 schools, for a maximum of nine incidents per institution. Members of the research team collected information, in person, from each of the respondents for all retrospective incidents. The electronic CIFAC instrument allowed researchers to collect data on computer-related incidents serially, with up to three incidents being collected from each respondent.

1. CIFAC Questions

Respondents were read the definition of incident as given in III(c)1. They were asked to describe the incident on which they were reporting. They were asked to report “how serious” the incident was using the previously
explained Likert scale. After rating the seriousness of the incident, respondents were asked to explain why they had selected this rating. They were then asked to identify the primary focus of the incident.

Next, respondents were asked a series of questions related to what factors might have prevented the incident. They were asked to rate each factor, using the Likert scale detailed above, on its importance in preventing the incident. These questions fell into seven broad categories. Respondents were asked to judge the importance of:

1. increased resources such as personnel, hardware, software, networks, physical security, and access control tools;
2. increased training or education for various groups such as IT managers, IT staff, non-IT staff, faculty, students, and authorized external users;
3. having improved procedures for such things as network management, incident response, backup and recovery of systems and data, documenting systems and networks, auditing systems, configuring software, detecting and patching software bugs;
4. backup and recovery, documentation, promulgation of documentation and policies, logging, analysis of logs, and identification, authentication and authorization processes;
5. increased requirements for IT managers, IT staff, use of institutional resources, and use of personal information;
6. the level of knowledge of faculty, students, non-IT staff, and authorized external users; and,
7. improved configurations for networks, desktop software, desktop hardware, server or mainframe hardware, and server or mainframe software.

The instrument then asked a parallel series of questions relating to the cause of the incident. In addition, respondents were asked to judge the importance of:

1. accidental or careless behavior of IT managers, IT staff, non-IT staff, faculty, students, authorized external users, and unauthorized external users in causing the incident; and,
2. malicious or abusive behavior of the same groups of people in causing the incident.

Data were collected on the adequacy and effectiveness of pre-established incident response procedures at each institution as they related to each incident. The instrument further solicited input from respondents as to what stimulated them to act in response to incidents by asking them to rate the importance of the following in determining how and when to respond to the incident: cost to department, college or university; time involved for resolution; number of people affected; level, status, or rank of people affected; number of machines affected; type and sensitivity of data involved; type of machines affected; probability of further access or damage; probability of damage to individuals; and probability of damage to institutional reputation. Finally, the instrument gave each respondent an opportunity to identify and share with colleagues a best practice for preventing the incident, for mitigating the effects of the incident, and, for managing the incident.

2. Collection Methodology

As previously discussed, data were collected using SPSS Data Entry 4.0. Researchers made frequent backups of collected data, which have since been encrypted or destroyed. Upon return to Ann Arbor from each data collection trip, research team members gave an electronic copy of all collected data to the project statistician who uploaded the data to the SPSS database, inspected them for entry errors, and prepared the data for analysis.

Between the collection of retrospective data and the end of data collection on March 17, 2005, current incident data were collected from participants. Participants were invited to call the project any time after their initial interview through March 17 to report information relative to current incidents. The response to data collection was outstanding: data were reported on 69 current incidents and even after the dataset was closed, several participants offered to provide data on other new incidents.

When we closed the data set, information on a total of 319 incidents had been collected, 250 of which were retrospective and 69 of which were current.
3. Retrospective and Current Sample Pooling

After the collection of the current incidents, researchers wanted to determine whether all 319 incidents could be treated as one sample or whether the current and retrospective incidents needed to be analyzed separately as discrete samples of different phenomena. It was possible that, since the current incidents were culled from a much shorter time frame, they might be less severe or they might be of a different focus. Were respondents remembering the most serious incidents when they recalled and reported the retrospective incidents? Were the current incidents more frequent and less serious in type? Researchers explicitly reminded many of the respondents that reported incidents need not be “showstopper” incidents and that we were interested in collecting information on a wide variety of incident.

Incident seriousness was tested to determine whether it was the same between the retrospective and current samples. The mean seriousness ratings for retrospective and current incidents were 3.15 and 2.99, respectively, with variances of 0.721 and 0.826. Confidence intervals ($\alpha = .05$) were constructed for each sample; they were found to overlap, indicating that the null hypothesis that retrospective and current incidents were of the same seriousness could not be rejected.

Researchers then tested whether the foci of the incidents were broadly similar or dissimilar using two different tests. First, we tested whether the proportion of incidents in each sample focused on each category of incident was the same. For each of the three types of incidents, we found that the 95% confidence intervals constructed for the percentage of each type of incident overlapped between the current and retrospective incidents, indicating that there were no statistically significant differences in incident focus between the current and retrospective incident samples. In order to verify this assertion, we undertook a Mann-Whitney test, which also showed that there was no statistically significant difference between the foci of the two samples.

Based on these results, researchers decided that analysis of the data set would be undertaken on a pooling of the current and retrospective.
V. Analyses and Findings

Analyses and findings of the CIFAC study will be described in four sections. Section A provides a general description and discussion of the CIFAC data including information about some of the secondary questions in the instrument. Section B provides a description and analysis of the cause and prevention questions in the instrument. Section C addresses the instrument question dealing with the concept introduced by our focus group participants as “thresholds” and titled “stimulus to action” in the CIFAC study. Finally, section D looks at responses to the request for best practices and the analyses of these responses.

A. General Data Description

1. Institutions

Was there a balanced collection of incident data from different type and size institutions?

Data on 319 incidents were provided by 90 respondents at 36 colleges and universities. Inspection of the data set showed that approximately 36% of the incidents came from western schools, 46% from southern schools, 101 from Midwestern schools, and 117 from eastern schools. Approximately 63% of the collected incidents came from the large institutions, and 37% from the small/medium institutions. Fifty-seven percent came from public and 43% from private schools. Researchers found a good balance of data provided from public and private schools and a relatively good balance of incident data provided from large and small/medium institutions.

![Chart 2](image)

2. Seriousness Ratings

Were incidents provided reflecting different levels of seriousness?

Only 2% of the incidents reported were considered not at all serious. Twenty-six percent were considered somewhat serious, 31% quite serious and 41% extremely serious. Researchers considered this distribution to be good for continued analyses since no loading of incidents at any one seriousness level seemed to be occurring.
Did the geographical location of the respondents affect the seriousness ratings they gave for the incidents on which they reported?

Researchers did not find a significant relationship between seriousness ratings and the geographical regions of participant schools, leading us to conclude that no one region contributed a disproportionate quantity of incidents at any one level of seriousness. The balance and stability in the overall CIFAC data set relative to seriousness ratings strengthens the CIFAC study.

3. Incident Focus

Were incidents provided in each of the incident foci categories – people, systems, data?

Results showed a relatively balanced distribution across the three incident foci: 29.3% of the incidents were categorized by the respondents as people-focused, 26.5% as data-focused, and 44.2% as systems-focused. Even though researchers collected incidents from up to three different participants at each institution, and even though participants were free to select any incidents they wanted to report and individually identified the incident focus, the final sample reflected a good distribution between the three categories of incidents.
Did incidents of a particular focus come from one region more than another?

Researchers did not find a significant relationship between focus of the incident and the geographical regions of participant schools, leading us to conclude that no region produced a disproportionate number of incidents of any particular type.

Did incidents of a particular focus come from institutions of one type (public v private) or one size (large v small/medium)? Do size and type of institution affect the focus of incidents given to CIFAC?

Researchers did not find a significant relationship between people-focused incidents and institutional size or type. Likewise, they did not find a significant relationship between system-focused incidents and institutional size or type. They did find a slightly significant relationship ($\chi^2 (2) = 11.49, p = .003$) between data-focused incidents and institutional type with more data focused incidents coming from public institutions.

The balance and stability in the data set relative to incident focus and seriousness ratings strengthens the inferential potential of later analyses.

4. Regarding State Data Protection Laws

Was there a relationship between the frequency with which participants identified incidents of a particular focus and the state data protection laws impacting their institution?

Researchers found that the stringency of state data protection laws did not seem to significantly impact the percentage of data-focused incidents more than the systems or the people-focused categories.

Did participants identify incidents as more serious if they came from states with more stringent data protection laws?

Researchers found a weak but significant relationship ($r = .133, p = .018$) between seriousness ratings of incidents and stringency of data protection laws. Participants in states with more stringent data protection laws saw data-focused incidents as being slightly more serious than participants in states with lower data protection laws. The impact, while statistically significant, was relatively minor.

Was there a relationship between the stringency of state data protection laws and the stimuli to action as reported by respondents?

Researchers found that the stringency of data protection laws in a state had a minimal effect on participant’s selection of stimulus to action items and insufficient for interpretation. However, there were three stimuli to action that were significantly correlated with stringency of data protection: cost to department/institution ($r = .166, p = .003$); time involved for resolution ($r = .145, p = .010$); and number of people affected ($r = .127, p = .026$). This makes sense in light of the fact that many data protection laws include disclosure clauses that trigger increased cost, require time for documentation and notification, and being under the scope of the incident individuals who may not have been directly affected but whom institutions are still legally obligated to notify.

It can be concluded that the existence of increasingly stringent data protection laws seems to have no special effect on the study respondents, in terms of the incident focus, perceived incident seriousness, or the stimulus to action for the respondents. It is possible that our respondents were unaware of the data protection laws, that such laws are poorly communicated, or that such laws were felt to have very little relevance for the kind of incidents being reported to the CIFAC study. Without knowing more about the level of awareness our respondents had relative to data protection laws and the extent to which such laws are referenced in relation to institutional policies, we cannot draw meaning from these results.
5. Adequacy of Procedures and Responses

*How adequate did respondents say their procedures are?*

Many of our sample respondents indicated that their institutions did not have procedures in place for handling some of the incidents that were occurring. In 40% of the incidents, respondents said that their procedures were either not in existence, or were “not at all or only somewhat” adequate. Generally, if procedures were in place at the time of the incident, they were “quite or extremely” well followed (81% of incidents) and were felt to be “quite or extremely” effective (69% of incidents).

6. Size of Institution and Centralization of Services

*Does the size of the institution affect the centralization of services?*

One of the questions we asked each respondent was to quantify the overall degree to which systems and services were centralized at their college or university. Researchers, using nonparametric correlations (Spearman’s rho), found a high negative correlation between the institution enrollment figures as previously defined and the centralization of services \((r = -.570, p < .001)\). They did not find significant correlation between type of institution (i.e.: public versus private) and centralization of services when controlling for the size of the institution. To summarize, larger schools tend to have less centralization of services, but there is no relationship between centralization and whether the school is public or private.

7. Involvement of Interdepartmental Teams in Incident Management

*Do institutions have policies or practices that require people from different roles within the institution to be involved in computer-related incident management?*

Researchers asked each respondent if there are “unwritten institutional or organizational norms that require IT personnel, for certain kinds of incidents, to involve any of the following types of people: risk managers, attorneys, auditors, law enforcement, human resources, public relations, student affairs staff?” The question was repeated asking if there were written policies that require the involvement of such people.

Respondents responded in the affirmative with the following frequencies: attorneys, 76%; student affairs staff, 80%; law enforcement officials, 79%; and human resources personnel, 72%. These percentages fell dramatically when the questions specified “written policies” to 43%, 49%, 56%, and 51%, respectively. Respondents frequently indicated that they did not know if there were written policies in place.

The two lowest scoring roles for involvement in responding to computer related incidents were risk managers and auditors, with only 20% and 24% of respondents indicating that they had written policies in place for the involvement of these groups.

The confusion that surrounded these questions in many respondents’ minds indicates that the only conclusion that researchers can draw from these data is that there is substantial lack of awareness and some confusion surrounding the role of different institutional actors in responding to incidents. The fact that many respondents were unsure of which offices and persons to contact when responding to incidents indicates that colleges and universities should improve their policies regarding interdepartmental incident response and make sure that these policies are clearly promulgated to incident first responders.

B. Description and Analysis of the Prevention and Cause Questions

In analyzing the CIFAC data, researchers used descriptive statistics, frequency statistics, and bivariate analyses. The bivariate tests employed cross-tabulation chi-square, Kendall’s tau-b statistics, Spearman’s rho, and Pearson bivariate correlation statistics. Concurrently, we conducted analysis of the qualitative responses in the
questionnaires. The results of analyses having to do with the prevention and cause questions are discussed in the following:

1. Regarding Incident Prevention

What did respondents perceive as important in preventing incidents?

For 61% of the incidents reported, participants felt that the increased availability of access control tools was “somewhat,” “quite,” or “extremely” important to preventing the incident. For 19% of incidents it was felt to be extremely important. Increased availability of personnel was felt to be important to preventing the occurrence of 62% of the incidents with most seeing it as only “somewhat” important. It appears that more hardware, software, or network resources are not generally seen to be significant in preventing incidents.

However, increased availability of training and education was felt to be important in a large percentage of incidents. To prevent the incidents, training and education was felt to be important for IT managers in 70% of incidents, for IT staff in 76% of incidents, for non-IT staff in 68%, for faculty in 56%, and for students in 61% of the incidents. It was felt to be “extremely” important for non-IT staff in 26% and for students in 27% of the incidents reported. This emphasis on the importance of education and training is seen repeatedly in the CIFAC data and will be further discussed later in this report.

In preventing incidents, respondents felt that the existence of policy was by far the most important single issue. In 29% of incidents it was felt to be “extremely” important, in 30% “quite” important and in 23% “somewhat” important. Overall, respondents rated the existence of policy as important in preventing 81% of the incidents. Having sound policies in place, following them, and having them well known and understood through education and training, are points that are repeatedly illustrated in the data and will be further discussed in this report.

2. Regarding Incident Cause

What did respondents perceive as important in causing computer-related incidents?

A lack or deficiency in education or training for IT staff and for non-IT staff was felt to be important in causing 55% and 53% of incidents, respectively. Increasing requirements for the use of institutional resources was also felt to be important; the lack or deficiency of such requirements were felt to be important as a cause in 54% of the incidents.

One area that is not seen as important in causing a high percentage of the incidents that were reported is the lack of or deficiency in back-up procedures. This indicates that the backup resources and procedures are well-established and securely in place for our participating institutions or they were not considered important for the incidents that were reported to CIFAC.

3. Regarding Accidental or Careless and Malicious or Abusive Behaviors

Which group’s accidental or careless behaviors were perceived important in causing incidents?

Incidents identified by respondents as having been caused by “accidental or careless” behavior seem to focus on the behaviors of students, non-IT staff and IT staff most frequently. “Accidental or careless” behavior of students was felt to be important as a cause in 38% of the incidents; for non-IT staff it was 36%, and for IT staff it was 32%.

Which group’s malicious or abusive behaviors were perceived important in causing incidents?

Of the incidents reported, “malicious or abusive” behavior of students or of unauthorized external users (i.e.: hackers) is perceived as “somewhat, quite or extremely” important in 29% of the cases for students, and in 35%
of the incidents for unauthorized external users. For each of these groups, such behavior, when perceived to be a cause of the incident, was rated as being “extremely” important in a majority of cases.

4. Relationships Among Prevention and Cause Variables

Next researchers asked, are there certain responses to the prevention and cause questions that seem to be related? That is, when one response is given as important, is another response given as important as well at a statistically significant frequency? Are certain causal factors as given by our respondents associated with certain preventative factors?

We found that some variables in our instrument were highly correlated between prevention and cause. If a variable was cited as an important cause of incidents, such as “too little knowledge required of students prior to the use of systems,” its logical counterpart (increased education for students) was likely to be cited as important for prevention. Seeing high correlations between some variables, we explored these relationships for further meaning.

Were answers to the prevention questions and their same-type cause questions alike?

Researchers found, as expected, that there was significant correlation between all the cause and prevention same-type questions, and, in most cases, those correlations were significant at the 0.01 level (2-tailed). This was interpreted to mean that cause and prevention were highly related (like two different sides of the same coin) in the minds of our respondents. It also lent validity to the construction of the CIFAC instrument. Although in many cases, the correlation coefficient between these cause and prevention same-type questions was above 0.7, further analysis rejected collinearity as significantly causing any aberrations in the data.

Researchers saw the correlations between factors in the areas of prevention and cause. They also observed the way respondents reflected the perceived importance of related variables in explaining what would have prevented an incident and what they felt was important in causing an incident. They pursued further analysis to discover if underlying relationships could be identified and named.

5. Factor Analysis

Are there factors that explain the participants’ responses?

Our survey instrument generated a large number of variables. This plethora of information is a barrier to the generation of parsimonious analyses. Thus, it was decided to utilize statistical data reduction techniques to identify relationships between the variables in the section of the survey related to the inquiry on cause and prevention of incidents.

We conducted an exploratory factor analysis to determine if there are possible underlying factor structures. This technique helped us to create groupings of variables that reflect common and unique differences of the variables in the groupings. Initially, we employed factor analysis to find associations between different variables in our data set. This procedure was applied to the data set as a whole and to the subgroups of prevention and cause variables. In all three cases a better explanation of the differences for the four factor groups was revealed.

In the second round of computations, four factors were specifically selected for extraction because together they explained 42.72% of the variance. This helped us select those variables that could then be removed to reduce the data to a smaller group of variables. Since the prevention and cause questions numbered 87 variables, we used very stringent criteria in the computational code, suppressing low loading coefficients. (See Appendix E for more documentation on the factor analysis process and for tables of results.)

Researchers found that four factor groups were responsible for most of the responses we were getting from participants. We have named these factors groups “IT personnel,” “Academic Users,” “Networks,” and “Non-IT Staff,” according to the object of their associated variables.
In each of the four factors, the variables represent distinctive and separate characteristics:

<table>
<thead>
<tr>
<th>Group</th>
<th>Object</th>
<th>Associated Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IT Personnel</td>
<td>Education, Requirements, Accidental Behavior</td>
</tr>
<tr>
<td>2</td>
<td>Academic Users</td>
<td>Education, Knowledge, Accidental Behavior</td>
</tr>
<tr>
<td>3</td>
<td>Networks</td>
<td>Resources, Procedures, Configuration</td>
</tr>
<tr>
<td>4</td>
<td>Non-IT Staff</td>
<td>Education, Requirements, Knowledge, Accidental Behavior</td>
</tr>
</tbody>
</table>

Researchers found that these underlying characteristics are similar in the specific variables loading in each of the factors. The variables loading in three of the four factors are associated with human behaviors and people-related issues: Education, Requirements, Knowledge, Accidental Behavior.

It is important to note that, as indicated previously, when asked to identify the incident focus for each reported incident, respondents assigned a similar number of incidents to each of the people and data categories and a larger number of incidents to the systems category. This distribution of incident types was stable across different types of institutions. Yet, when respondents were asked to assign importance to variables relating to cause and prevention, their responses shown above indicate that mainly people-related factors, and to a lesser degree system-related factors, were identified as the relevant elements. Elements characterized as data factors were largely disregarded. That is, when respondents were asked to indicate the incident focus, they identified people-, data-, and systems-focused incidents. However, when they thought about preventing the incidents and about their causes, they responded to CIFAC questions by identifying mostly people-related factors and some systems-related factors.

6. Reliability Analysis

Do the answers to the questions in each of these four factor groups reflect the differences in the respondents? Or is the variation in the responses due to possible errors in the construction of the survey?

The variables comprising each factor group were analyzed for strength of relationships. Only those variables with the highest loading coefficients became part of the averaged scales created for each factor. Subsequently, Cronbach’s Alpha was computed as a measure of reliability, or internal consistency. The two scales with the greatest number of items needed to be divided by creating subscales. The first set of subscales comprised those variables related to IT staff and IT managers. Three IT personnel subscales sum up common variability of prevention and cause for education, requirements and accidental behavior. The second set of subscales related to academic users, with groupings of education and of knowledge variables for faculty and students. For each of the resulting scales and subscales the summary statistic Cronbach’s alpha was above 0.700, lending validity to the scales’ construction (see Appendix E).

These scales represent a first attempt at generating a score to guide the analysis of computer incidents.

7. Cluster Analysis

As part of the process of determining if there were underlying factor group structures in the prevention and cause variables, scores were computed for each factor group and saved for use as input variables in cluster analysis. These scores were based on the correlation of each variable with each factor group. That is, those variables with the greatest association will tend to collect in a factor group that would highlight some common characteristic, such as in the importance assigned to education of IT personnel both as variables measuring prevention and cause.

Each incident has a score based on each of the factor groups. Employing agglomerative Q-Type hierarchical cluster analysis methods on the factor group scores, we clustered the incidents through these scores. This
technique facilitates the performance of subsequent analyses. Incidents in each cluster are identified by their title. While only titles are referenced, we believe that the general nature of the incident is sufficiently reflected by the title to give the reader a sense of the incidents included in a given cluster (incidents by cluster membership are included in Appendix D of this report).

Subsequently, cluster membership was assigned as a variable for analysis of variance (ANOVA) to perform post hoc multiple comparisons, as means to reveal common characteristics of the incidents in each cluster. These results serve to characterize the differences and similarities amongst the clusters of incidents. On average, respondents assigned high rating of importance to number of people affected, type of data involved, probability of further access or damage, and probability of damage to institutional reputation. These analyses can be reviewed in greater detail in Appendix E.

8. Contrast of Stimulus to Action Responses by Cluster Membership

The multiple comparison technique was employed in the contrast of stimulus to action responses by cluster membership. This is the final step in the sequence of analyses of the prevention and cause sections of the CIFAC study. At this point, the statistical clustering of incidents revealed significant differences (p<0.05; 2-tailed) in the level of importance between specific stimuli to action by clusters, as can be seen in table xxx. The number of people affected and the probability of damage to persons were categorized as important stimuli to action in all clusters; though in cluster 1, the probability of damage to persons was given a significantly higher degree of importance than in the other clusters. The number and type of machines were also a relevant stimulus for the clusters, though far more so for cluster 4 than for the others involved. It could be said that the incidents in clusters 1 and 2 assign greater importance to people issues, while in clusters 3 and 4 system issues share importance with people issues.

<table>
<thead>
<tr>
<th>STIMULUS TO ACTION</th>
<th>CLUSTER 1</th>
<th>CLUSTER 2</th>
<th>CLUSTER 3</th>
<th>CLUSTER 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean (SD)</td>
<td>Mean (SD)</td>
<td>Mean (SD)</td>
<td>Mean (SD)</td>
</tr>
<tr>
<td>Cost to Department</td>
<td>1.83(1.13)</td>
<td>1.94(0.97)</td>
<td>1.86(0.98)</td>
<td>2.08(1.25)</td>
</tr>
<tr>
<td>Time Involved for Resolution</td>
<td>2.00(1.07)</td>
<td>2.20(1.13)</td>
<td>1.86(1.13)</td>
<td>2.42(1.14)</td>
</tr>
<tr>
<td>Number of People Affected</td>
<td>2.49(1.20)</td>
<td>3.06(1.07)</td>
<td>2.75(1.18)</td>
<td>2.94(1.19)</td>
</tr>
<tr>
<td>Rank of People Affected</td>
<td>2.22(1.31)</td>
<td>2.03(1.15)</td>
<td>1.89(1.15)</td>
<td>2.43(1.25)</td>
</tr>
<tr>
<td>Number of Machines Affected</td>
<td>1.45(0.89)</td>
<td>1.89(1.03)</td>
<td>2.18(1.19)</td>
<td>2.52(1.29)</td>
</tr>
<tr>
<td>Type of Machines</td>
<td>1.42(0.91)</td>
<td>1.66(0.88)</td>
<td>1.39(0.66)</td>
<td>2.02(1.14)</td>
</tr>
<tr>
<td>Type of Data Involved</td>
<td>2.95(1.22)</td>
<td>2.86(1.11)</td>
<td>2.61(1.22)</td>
<td>2.56(1.32)</td>
</tr>
<tr>
<td>Prob of Further Access/Damage</td>
<td>2.74(1.24)</td>
<td>2.98(1.16)</td>
<td>2.95(1.20)</td>
<td>3.21(1.00)</td>
</tr>
<tr>
<td>Prob Damage to Persons</td>
<td>2.53(1.26)</td>
<td>1.72(1.12)</td>
<td>1.73(1.11)</td>
<td>1.87(1.25)</td>
</tr>
<tr>
<td>Prob Damage to Institutional Reputaion</td>
<td>2.87(1.14)</td>
<td>2.64(1.03)</td>
<td>2.52(1.91)</td>
<td>2.79(1.07)</td>
</tr>
</tbody>
</table>

Mean rating of importance, values from 1-not important up to 4-extremely important

Significantly different (p < 0.05; 2-tailed):

a contrasted to cluster 1
b contrasted to cluster 2
c contrasted to cluster 3.
9. Summary Regarding Factor Analysis

*What can we conclude from these analyses?*

Researchers have concluded from the incidents reported to us in the CIFAC study that there are specific factors perceived to be related to the occurrence of various clusters of computer-related incidents. For the factors that are related to IT personnel, it appears that more education and training, more requirements as to how they perform their jobs, and procedures that help prevent them from accidental or careless behaviors are important in preventing the incidents with higher scores in these factors.

For the factors that are related to users, it appears that more education and awareness training, more stringent requirements, and better knowledge prior to use of systems would be helpful in preventing them from accidental or careless behaviors and preventing the incidents associated with these factors.

For factors related to networks, more resources, procedures, and requirements relative to configuration of software and hardware, would be helpful in preventing the incidents associated with these factors from happening.

For factors related to non-IT staff, more education, more requirements, and more knowledge prior to use of systems would help to prevent the accidental behaviors that are associated with the incidents related to these factors.

It is very important to note that even though there was a good distribution of incidents in different foci, in the overall CIFAC data set, when respondents were asked about prevention of incidents and cause, three of the four factors that came out of the analysis dealt with people, none dealt with data, and only one dealt with systems. CIFAC respondents identified approximately 29.3% of the reported incidents as people-focused incidents when they were asked to categorize the incidents. However, they attributed much more importance to people-related factors when they thought about and rated the importance of certain factors for prevention or as the cause of the incident. They identified education, training, requirements, more knowledge prior to use of systems, and procedures as important for preventing multiple clusters of incidents and the lack or deficiency of these items as associated with the cause of the incidents.

C. Description and Analysis of Stimulus to Action Question

From discussions in the focus groups and from previous research, the CIFAC staff identified a set of ten variables that they thought might be of varying importance in causing individuals to respond when an incident occurred. They called these variables “stimuli to action” and hypothesized that if they could identify associations between the variables, certain types of incidents, seriousness of incidents, and other factors, perhaps recommendations could be made that would help the field respond and even diminish the effects of certain types of incidents. The variables were:

- Cost to department, college/university
- Time involved for resolution
- Number of people affected
- Level, status, or rank of people affected
- Number of machines affected
- Type and sensitivity of data involved
- Type of machine(s) affected
- Probability of further access or damage
- Probability of damage/harm to persons
- Probability of damage to institutional reputation

Researchers asked each participant to rate, on the scale used throughout the study, the importance of each variable as a stimulus to action for them relative to the incident being reported.
1. Stimulus to Action and Institutional Size

*Were certain stimuli to action more important to respondents from institutions of different sizes?*

Researchers found that only one variable, the number of machines affected, had a statistically significant (r = -.117, p = .040) inverse relationship with size of institution. The number of machines affected was more important as a stimulus-to-action for respondents from smaller institutions than for those from the larger institutions, although at a low enough value to be of little meaning.

2. Stimulus to Action and Institutional Type

*Were certain variables more important as stimuli to action to respondents from public and private institutions?*

Results showed a significant negative correlation between type of institution (a dummy variable defined as public = 1 and private = 0) and the number of people affected as a stimulus to action (r = -.126, p = .027.) That is, respondents from private institutions felt that the number of people affected was a stronger stimulus to action than those respondents from public institutions. Results also showed a positive correlation between type of institution and the type and sensitivity of data (r = .123 , p = .031) as well as the probability of damage to persons as stimuli to action (r = .127, p = .025). Respondents from public institutions felt that the type of data and the probability of damage to persons was a more important stimulus to action than did respondents from private institutions.

3. Stimulus to Action and Seriousness Ratings

*Were certain stimuli to action associated with different seriousness ratings given by respondents?*

Researchers found significant correlations between all of the stimuli to action and seriousness ratings except for the stimulus to action called “type of machines”. Therefore they grouped the stimuli to action by common characteristics and found that three of the stimuli significantly explained the variation in the ratings of seriousness—“probability of damage to institutional reputation (t = 1.971, p = .050), number of people affected (t = 6.015, p < .001) and probability of damage to persons (t = 2.765, p = .006). Perceptions of the seriousness of an incident were affected by the probability of damage to institutional reputation, number of people affected, and/or probability of damage/harm to a person.

*Do individuals in different roles perceive same incidents at the same levels of seriousness and is there a pattern to the rationales they give for their ratings?*

Recall that during the early focus group exercises used to formulate concepts and guide the design of the CIFAC study, participants were asked to rate the seriousness of six briefly described incidents and give their rationale for their ratings. Additionally, during the larger study, participating institutions’ CIOs were asked to rate the seriousness of four of the six briefly described incidents (“Fire in the Data Center,” “Death Threat,” “So Close Yet So Far,” and “US Secret Service”) and to also provide the rationales for their ratings. (See Appendix G for copies of these incidents.)

Researchers found that focus group respondents rated four of their incidents, including those titled “Fire in the Data Center” and “Death Threat” at means of 3.45 and 3.39, respectively. Respondents rated the other two incidents much lower; “So Close Yet So Far” was rated at a mean of 2.85 and “US Secret Service” was rated the least serious of the incidents with a mean rating of 1.82. To try to discover what made the higher scoring seriousness group of four incidents different from the two lower seriousness incidents, a content analysis was performed. As discussed in section II.A.2, Researchers found that the two sets of incidents differed primarily due to three variables:

1. quantity or extent of loss
2. importance or level of people involved or potentially involved, and
3. potential for further damage, access, or danger.

The following table shows the seriousness ratings given by the CIFAC study CIOs compared with those given the focus group participants.

<table>
<thead>
<tr>
<th>Incident Titles</th>
<th>Mean Seriousness Ratings (Standard Deviation)</th>
<th>CIOs</th>
<th>Focus Group Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire in the Data Center</td>
<td>3.70 (.54)</td>
<td>3.45</td>
<td></td>
</tr>
<tr>
<td>Death Threat</td>
<td>3.60 (.67)</td>
<td>3.39</td>
<td></td>
</tr>
<tr>
<td>So Close, Yet So Far</td>
<td>3.33 (.72)</td>
<td>2.85</td>
<td></td>
</tr>
<tr>
<td>US Secret Service</td>
<td>2.13 (.57)</td>
<td>1.82</td>
<td></td>
</tr>
</tbody>
</table>

Table 6

There was agreement among the CIOs as to the seriousness of each of the incidents they reviewed, and there was agreement between the CIOs and the focus group participants as to the seriousness of these four incidents. Using a student’s t-test, researchers concluded that we can be confident, at the 95% level, that other CIOs in the general population would rate these incidents in the same way.

While time did not allow further analyses of these results or the rationales provided by the CIOs for their seriousness ratings, inspection of these statements shows that some of the same variables repeatedly appear: potential damage/harm to individuals, extent of damage or potential damage, and level of persons involved. Appendix G provides a listing of CIO rationales for seriousness ratings.

4. Stimulus to Action and Incident Type

Were certain stimuli to action associated with different foci of incidents? Were some more important for one type of incident than another?

Cramer’s V measures of association based on chi-square tests between stimulus to action variables and incident type showed that all were significantly related at \( \alpha \leq .05 \) with the exception of “level, status, or rank of people affected.” That is, how important the respondents in the CIFAC study ranked each of the stimuli to action variables was significantly associated with the focus of incident being rated, with one exception.

<table>
<thead>
<tr>
<th>STIMULUS TO ACTION</th>
<th>CRAMER’S V MEASURE</th>
<th>SIGNIFICANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost to college, department, university</td>
<td>.186</td>
<td>.002</td>
</tr>
<tr>
<td>Time involved for resolution</td>
<td>.179</td>
<td>.003</td>
</tr>
<tr>
<td>Number of people affected</td>
<td>.247</td>
<td>.001</td>
</tr>
<tr>
<td>Level, status, or rank of people affected</td>
<td>.111</td>
<td>.266</td>
</tr>
<tr>
<td>Number of machines affected</td>
<td>.335</td>
<td>.001</td>
</tr>
<tr>
<td>Type of machines affected</td>
<td>.221</td>
<td>.001</td>
</tr>
<tr>
<td>Type and sensitivity of data involved</td>
<td>.281</td>
<td>.001</td>
</tr>
<tr>
<td>Prob. of further access or damage</td>
<td>.150</td>
<td>.032</td>
</tr>
<tr>
<td>Prob. of damage to persons</td>
<td>.347</td>
<td>.001</td>
</tr>
<tr>
<td>Prob. of damage to institutional reputation</td>
<td>.146</td>
<td>.041</td>
</tr>
</tbody>
</table>

Table 7: Stimulus to Action by Type of Incident

The Cramer’s V merely told us, however, if there would be significant differences in the seriousness of each stimulus depending on focus; it did not indicate between which foci these differences might be. Therefore, researchers performed a chi-square analysis on each contingency table with focus in the columns and
importance of the stimuli to action in the rows. The data set was divided into three subsets dependent on incident focus. The SPSS t-test function was used to construct a 95% confidence interval for the mean of each stimulus-to-action rating on each subset. We found that, with the exception of the “level, status, or rank of people affected” variable, which had previously been identified as not significantly different between the different foci, there were statistically significant differences between the ratings of the stimuli to action between at least two foci.

The results of our analysis, for each stimulus to action item identified on the instrument, are as follows:

1. “Cost to department, college, or university” was more important in systems-focused incidents than in data-focused incidents.
2. “Time involved for resolution” was more important in systems-focused incidents than in data-focused incidents.
3. “Number of people affected” was more important in people and systems-focused incidents than in data-focused incidents.
4. “Number of machines affected” was more important in systems-focused incidents than in people- and data-focused incidents.
5. “Type of machines affected” was more important in systems-focused incidents than in people-focused incidents.
6. “Type and sensitivity of data involved” was more important in people-focused incidents than data- and system-focused incidents.
7. “Probability of further access or damage” was more important in people-focused incidents than in data-focused incidents.
8. “Probability of damage to persons” was more important in people- and data-focused incidents than in systems-focused incidents.
9. “Probability of damage to institutional reputation” was more important in people-focused incidents than in data-focused incidents.

As the Cramer’s V test predicted, “level, status, or rank of people affected” did not show up as an important stimulus-to-action for any of the subsets based on incident focus.

Every stimulus to action showed equal to or less seriousness, at a statistically significant level, for data-focused incidents than for people- or systems-focused incidents. There was only one exception to this: “probability of damage/harm to persons.” Indeed, for almost every stimulus to action, data incidents had a lower mean score than both people and data incidents. This seems to indicate that data incidents are substantially different from people or systems incidents. This will be discussed further as the CIFAC categorization scheme is reflected upon in section VII of this report.

Researchers concluded that our respondents were moved to action most by three potential stimuli: probability of damage to institutional reputation, probability of danger to individuals, and numbers of machines affected. Unlike the responses from our focus group participants, and to some extent from the CIOs, regarding the importance of level, status, or rank of individuals affected in determining seriousness of the incident, our results show that level, status, or rank was not an important stimulus to action for CIFAC participants.

The importance of potential damage to institutional reputation, probability of danger to individuals, and large numbers of machines (extent of damage) has repeatedly shown up in the data as being important variables in determining seriousness and in moving participants to action. We suspect that differences in the perception of how important level, status, or rank is in moving one to action, depends on the role of the respondent. Those who deal more often with institutional level concerns may take the level, status, or rank of individuals involved in an incident more seriously anticipating potential effects on institutional reputation or anticipating administrative repercussions when the affected individual is of a higher rank. Those who deal with incidents on a daily basis and who see a wide range of incidents and effects, may not perceive, or respond as much to, the level, status, or rank of the individual affected as an important stimuli to action. Alternatively, this may reflect an unrealized but idealized image of the IT professional as a steward of computing services regardless of the political power of her client.
D. Description and Analysis of Best Practices Question

1. Preliminary Contextual Analysis of the Best Practice Responses

The CIFAC research staff asked each respondent, for each incident, to recommend to colleagues a “best practice” for preventing the incident they had described, for mitigating the impact of the incident, and for managing the incident. These responses were wonderfully thoughtful, freely shared, and in some cases very humorous. It seemed to us that this set of questions gave our respondents an opportunity to reveal the frustration they feel regarding the number of incidents that are happening, the continuous bugs and poor default settings in much COTS software, the persistent complaints regarding perceived and real copyright violations, the difficulty getting ahead of malicious-minded users, and the seemingly never-ending requirements for education and training because of fast moving and ever-changing technology and the inherently transient population of users in the academic setting.

Most professionals recognize that having policies and procedures and following them is important. Likewise, they realize that providing education and training is important for the skill sets of the IT people, for the general awareness of users, and for establishing knowledge about the acceptable limits of behaviors. However, we were not prepared for how important these foundational elements – policies, procedures, education and training – were to the participants in the CIFAC study.

*Did respondents recommend similar best practices for prevention, mitigation, and management across all incidents?*

The results of preliminary content analysis by members of the CIFAC research team on a random sample of half of the best practices volunteered by respondents showed that recommendations fell into two very similar categories for our tripartite question.

For prevention and for mitigation, respondents gave best practices in two most often recommended groupings that we have entitled “Foundational Practices” and “Technical/Security Practices”.

**Foundational Practices:** The most highly recommended best practices for prevention of incidents were education, training and awareness. The second highest ranking best practice for prevention of incidents was having and following policies and procedures. The most frequently recommended practices for mitigating incidents were straight-forward communication with affected individuals or groups and the establishment and use of interdepartmental communication and collaboration to handle the problem. Also recommended as desired best practices were “decisive and timely actions,” “having and following predetermined and established procedures,” and “education, training, and awareness.”

**Security/Technical Practices:** The most highly recommended best practices for prevention were: patching and debugging systems; the second highest recommendations were for implementing logging, analyzing logs, and monitoring systems. Also frequently recommended were: deploying firewalls, IDS/IPS systems, ensuring strong access control systems and passwords, requiring proper configurations and, employing automated quarantining procedures. For mitigation, the most frequently recommended best practices were straightforward communication with affected individuals or groups and the establishment and use of interdepartmental communication and collaboration to handle the problem. Also recommended as desired best practices were “decisive and timely actions,” “having and following predetermined and established procedures,” and “education, training, and awareness.”

To manage the incident, respondents gave best practices in two most often recommended groupings that we have entitled “Foundational Practices” and “Communications Practices.” Unlike recommendations in the areas of prevention and mitigation, there was no technical best practice grouping

**Foundational Practices:** The most highly recommended best practices were having and following pre-established procedures and having an inter-departmental incident response team already in place.
Communication Practices: The most highly recommended best practices were engaging in frequent and continuous communication with incident handlers, providing communication with the community regarding the incident (e.g.: the potential effects, what is being done, and what they might expect in the near future), and taking quick and decisive action (e.g.: knowing what to do, doing it, and communicating it).

2. Statistical Analysis of the Best Practice Responses

While preliminary contextual analysis of the responses CIFAC participants gave when asked for best practices were very interesting and surprisingly consistent in highlighting the importance of education, training, policies, procedures, direct communication with users, and quick security control responses, we wanted to find out if these responses would hold up when the recommended best practices were subjected to more rigorous statistical analysis.

To accomplish this, descriptive phrases or keywords were pulled verbatim from the best practice data to describe each of the best practices discussed. Recall that best practices were solicited from CIFAC participants for preventing the incident, for mitigating the effects of the incident, and for managing the incident. Two other open-ended questions that appeared earlier in the CIFAC survey instrument asked “If you could have done one thing to prevent this incident from happening, what would it have been” and “If you saw this incident starting again, what one thing would you do to mitigate the incident’s impact?” These two questions were also included in the next level contextual analysis.

For prevention, mitigation, and management, the five most frequently recommended categories of best practices were taken from the contextual analysis. None of the categories were limited or mutually exclusive; best practices could fall in none, one, or more than one category.

Three copies of the 319 incidents in the CIFAC database were produced for members of the CIFAC research team. Researchers read each incident description and independently determined the presence of any of the keywords that indicated a particular best practice response. When a staff member judged a best practice to be present, it was noted as being present. (See Appendix F for more information on this process.)

3. Inter-rater agreement

Was there agreement between the three CIFAC staff in their ratings of the incident best practices?

Researchers used Cohen’s kappa analysis to test reliability. Three kappa analyses were used because the team had three raters. They found that on all questions, the unweighted mean kappa value computed between all three respondents was at or above .462; the mean value was .672. This is considered “substantial” strength of agreement by one widely-cited interpretation of Cohen’s kappa results.11

Research raters agreed on 88.07% of their observations,12 with 9.30% of observations being rated as “present” by all raters and 77.68% of observations being rated as “not present” by all raters. The remaining 11.93% of observations were found to be present by one or two observers, but there was no unanimity. A best practice was found to be present if two or more of the raters believed that it was indicated by the respondent. Assured of

11 Landis, J.R. & Koch, G. (1977) “The measurement of observer agreement for categorical data.” Biometrics 33, 159-174. It should be noted that there is some controversy in the statistical literature surrounding the assignment of adjectives to Cohen’s kappa results, but levels of above .600 are widely considered to represent agreement at a non-trivial level from which conclusions can easily be drawn.

12 For the purposes of this analysis, “observation” means the thirty potential best practice categories for each incident. One of the six possible responses was “not present/does not know” and was not used in analysis.
agreement among raters, researchers were able to proceed to describe the best practice relationships with different variables within the study.

4. Regarding Best Practices and Incident Types

**Are certain best practices for (prevention, mitigation, management) associated with certain incident foci?**

A 3x2 cross-tab was run for each of the 18 best practice observations and a chi-square test was included to ascertain whether there was a relationship between a best practice and incident type.

Results showed that the most commonly given best practice for preventing, mitigating, and managing people- and data-focused incidents was education and training, with collaboration and communication being the next most frequently volunteered response. For preventing, mitigating, and managing systems-focused incidents, the most commonly given best practices were to test, patch, or debug; technically prevent or control the incident; remove or quarantine the cause; collaborate and communicate; and take decisive and timely action.

**Are certain best practices associated with preventing certain types of incidents?**

In the area of prevention best practices, researchers found three best practices that were significantly related to incident types: Education/training, test/patch/debug, and technical prevention and control.

Results showed:

1. The highest percentage of “education/training” best practices were given for people incidents and the lowest percentage for systems incidents; a significant difference between incident types ($\chi^2 (2) = 34.763, p < .001$).

2. The highest percentage of “test/patch/debug” best practices were given for systems type incidents, and the lowest for people type incidents; a significant difference between incident types ($\chi^2 (2) = 21.773, p < .001$).

3. The highest percentage of “technical prevention and control” best practices were given for systems type incidents and the lowest for people type incidents; a significant difference between incident types ($\chi^2 (2) = 15.714, p < .001$).

**Are certain best practices associated with mitigating certain types of incidents?**

In the area of mitigation best practices, researchers found two best practices that were significantly related to incident types, as might be expected: education and training, and removing or quarantining the cause.

1. The highest percentage of “education/training” best practices were given for people incidents and equal but lower percentages were given for systems and data incidents; a significant difference exists between incident types ($\chi^2 (2) = 7.368, p = .025$).

2. The highest percentage of “remove/quarantine cause” best practices were given for systems incidents, and the lowest and early equal percentages for people and data incidents; a significant difference between incident types ($\chi^2 (2) = 19.999, p < .001$).

**Are certain best practices associated with managing certain incident types?**

Researchers did not find significant relationships between any of the other best practices and incident types. All management best practices were seen to be normally distributed across all types of incidents; that is, there were no particular relationships for any one management best practice and a particular incident type. The best practices that were given for managing incidents were recommended as equally good for people-focused, system-focused or data-focused incidents.

---

13 “$\chi^2$” is the standard statistical abbreviation for chi-square. It is followed by an integer in parentheses that states the degrees of freedom.
Are certain best practices associated with the seriousness of incidents?

Researchers did not find any statistically significant correlations where the correlation between seriousness and the recommendation of a best practice was noteworthy (defined as $r \geq .150$). There appears to be no significant relationship between any of the best practices and the perceived seriousness of the incidents.

5. Relationships Between Best Practices and Identified Clusters of Incidents

Do respondents give certain best practices for certain clusters of incidents? Are the clusters found in analyses of CIFAC data related to certain best practices given by the respondents?

A statistical cross tabulation procedure was used to measure association with two-way tables of the clusters of incidents in columns, and each of the best practice variables (six for each of prevention, mitigation, and management) in rows. Because of the nominal nature of the clusters, a Cramer’s V measure based on chi-square tests was used to search for significance.

Researchers found that four of the best practices had relationships with the identified clusters of computer-related incidents: Education and training; testing, patching, and debugging; and technical controls were put forth as best practices for prevention. Quarantine and removal of causes was suggested as the best practices for mitigation.

That is, the common elements that were previously identified in the factors are the same common elements identified in the analysis of best practices given by the CIFAC respondents.

In summary, the best practices recommended by the study participants are unrelated to the size, type, and location of academic institutions. Similarly, the foci of incidents seem to matter little to the best practices recommended. That is, best practices for prevention, mitigation, and management of computer-related incidents are similar across all models and types of factor analysis, cluster analysis, and analysis of the stimuli to action.
VI. Summary of Findings

1. Seriousness Ratings Distribution
Only 2% of the incidents reported were considered not at all serious. Twenty-six percent were considered somewhat serious, 31% quite serious and 41% extremely serious. Researchers considered this distribution to be good for continued analyses since no loading of incidents at any one seriousness level seemed to be occurring.

2. Seriousness and Geography
Researchers did not find a significant relationship between seriousness ratings and the geographical region’s of participant schools, leading them to conclude that no one region contributed a disproportionate quantity of incidents at any one level of seriousness. The balance and stability in the overall CIFAC data set relative to seriousness ratings strengthens the CIFAC study.

3. Incident Focus-Distribution
Results found a relatively balanced distribution across the three incident foci. Twenty-nine percent of the incidents were categorized by the respondents as people-focused, 26% as data-focused, and 44% as systems-focused. Even though researchers collected incidents from up to three different participants at each institution, and even though participants were free to select whatever incident they wanted to report and individually identified the incident focus, the final sample was distributed between the three foci of incidents.

4. Incident Focus and Geography
Researchers did not find a significant relationship between focus of the incident and the geographical regions of participant schools, leading us to conclude that no region produced a disproportionate number of incidents of any particular type.

5. Incident Focus and Institutional Size and Type
Researchers did not find a significant relationship between people-focused incidents and institutional size or type. Likewise, they did not find a significant relationship between system-focused incidents and institutional size or type. They did find a slightly significant relationship (p = .002) between data-focused incidents and institutional type with more data focused incidents coming from public institutions.

6. Incident Focus and Data Protection Laws
Researchers did not find that the stringency of state data protection laws significantly impacted the percentage of data-focused incidents more than the systems- or people-focused categories.

7. Incident Seriousness and Data Protection Laws
Researchers found a statistically significant but unremarkable relationship (r = .133, p = .018) between seriousness ratings of incidents and stringency of data protection laws. Participants in states with more data protection laws saw data-focused incidents as being slightly more serious than participants in states with fewer data protection laws. The impact, while statistically significant, was relatively minor.

8. Stimulus to Action and Data Protection Laws
Researchers found that the stringency of data protection laws in a state had only a minimal effect on participants’ selection of stimulus to action items and is insufficient for meaningful interpretation. However, there were three stimuli to action that were significantly correlated with stringency of data protection: cost to department/institution (r = .166, p = .003); time involved for resolution (r = .145, p = .010); and number of people affected (r = .127, p = .026).

9. Adequacy of Procedures
Many of our sample respondents indicated that their institutions did not have procedures in place for handling some of the incidents that were occurring. In 40% of the incidents, respondents said that their procedures were either not in existence, or were “not at all” or only “somewhat” adequate. Generally, if procedures were in place at the time of the incident, they were “quite or extremely” well followed (81% of the incidents) and were felt to be “quite or extremely” effective (69% of the incidents).
10. Institutional Size and Centralization of Services
Researchers found a high negative correlation between the institution enrollment figures as previously defined and the centralization of services ($r = -.570$, $p < .001$). They did not find significant correlation between type of institution (i.e.: public or private) and centralization of services. To summarize, larger schools tend to have less centralization of services, but there is no relationship between centralization and whether the school is public or private.

11. Researchers found that respondents responded affirmatively when asked if institutional norms required the involvement of people with the following institutional roles: attorneys, 76%; student affairs staff, 80%; law enforcement officials, 79%; and human resources personnel, 72%. These percentages dropped when the questions specified written policies to 43%, 49%, 56%, and 51%, respectively. The two lowest scoring roles for involvement in responding to computer related incidents were risk managers and auditors, with only 20% and 24% of respondents indicating that they had written policies in place for the involvement of these groups.

12. Prevention: Increased resources
For 61% of the incidents reported, participants felt that the increased availability of access control tools was “somewhat,” “quite,” or “extremely” important to preventing the incident. For 19% of incidents it was felt to be “extremely” important. Increased availability of personnel was felt to be important to preventing the occurrence of 62% of the incidents, although most respondents saw it as only “somewhat” important. It appears that more hardware, software, or network resources are not generally seen to be significant in preventing incidents.

13. Prevention: Education and Training
Increased availability of training and education was felt to be important in a large percentage of incidents. To prevent the incidents, training and education was felt to be important for IT managers in 70% of incidents, for IT staff in 76% of incidents, for non-IT staff in 68%, for faculty in 56%, and for students in 61% of incidents. It was felt to be “extremely” important for non-IT staff in 26% of incidents and for students in 27% of the incidents reported.

14. Prevention: Policy
In preventing incidents, respondents felt that the existence of policy was by far the most important single factor. In 29% of incidents it was felt to be “extremely” important, in 30% “quite” important and in 23% “somewhat” important. Overall, respondents rated the existence of policy as important in preventing 81% of the incidents. Having policies in place, following them, and having them well known and understood through education and training, are points that are repeatedly illustrated in the quantitative and qualitative data.

15. Cause: Education and Training and Requirements
A lack or deficiency in education or training for IT staff and non-IT staff were felt to be important in causing 55% and 53% of incidents, respectively. Increasing requirements for the use of institutional resources was also felt to be important; the lack or deficiency of such requirements were felt to be important as a cause in 54% of the incidents.

16. Cause: Backup Procedures
One area that is not seen as important in causing a high percentage of the incidents that were reported is the lack of or deficiency in backup procedures. This indicates that backup resources and procedures are well-established and securely in place for our participating institutions or they were not considered important for the incidents that were reported to CIFAC.

17. Cause: Accidental or Careless Behaviors
Incidents identified by respondents as having been caused by the “accidental or careless” behavior seem to focus on the behaviors of students, non-IT staff and IT staff most frequently. “Accidental or careless” behavior of students was felt to be important as a cause in 38% of the incidents, for non-IT staff in 36% of incidents, and for IT staff in 32% of incidents.
18. Cause: Malicious or Abusive Behavior
Of the incidents reported, “malicious or abusive” behavior of students or of unauthorized external users (i.e.: hackers) was perceived as “somewhat, quite, or extremely” important in 29% of the cases for students, and in 35% of the incidents for unauthorized external users. For each of these groups, such behavior, when perceived to be a cause of the incident, was most often rated as being “extremely” important in the majority of cases.

19. Relationships Between Cause and Prevention Questions
Researchers found that there was significant correlation between related cause and prevention questions, and in most cases this correlation was significant at the .010 level (2-tailed).

20. Factor Groups Responsible for Variations in Responses
Four factor groups were found to be responsible for differences in responses from participants. We have named these factors “IT personnel,” “Academic Users,” “Networks,” and “Non-IT Staff” according to the object of their associated variables

In each of the resulting four factor groups, the variables represent distinctive and separate characteristics (see table 4).

21. Factors Related to IT Personnel
For the factors that are related to IT personnel, it appears that more education and training, more job requirements, and procedures that help prevent them from making accidental or careless mistakes are important in preventing the incidents associated with these factors.

22. Factors Related to Users
For the factors that are related to users, it appears that more education and awareness training, more stringent job requirements, and better knowledge prior to use of systems would be helpful in preventing them from accidental or careless behaviors, thereby preventing the incidents associated with these factors.

23. Factors Related to Networks
For factors related to networks, more resources, procedures, and requirements relative to configuration of software and hardware would be helpful in preventing the incidents associated with these factors from happening.

24. Factors Related to Non-IT Staff
For factors related to non-IT staff, more education, more stringent job requirements, and more knowledge prior to use of systems would help to prevent the accidental behaviors that are associated with the incidents related to these factors.

25. Stimulus to Action and Institutional Size
Researchers found that only the number of machines affected had statistically significant (r = -.117, p = .040) importance for institutions. The number of machines affected was slightly more important as a stimulus to action for respondents from small institutions than for those from the larger institutions.

26. Stimulus to Action and Institutional Type
Results showed a significant but unremarkable negative correlation between public status of an institution and the importance of number of people affected as a stimulus to action (r = -.126, p = .027.) That is, respondents from private institutions felt that the number of people affected was a slightly stronger stimulus to action than did respondents from public institutions.

27. Results showed a positive correlation between public status of an institution and the importance of type of data as stimulus to action (r = .123, p = .031) as well as the probability of damage to persons as a stimulus to action (r = .127, p = .025). Respondents from public institutions felt that the type and sensitivity of data involved and the probability of damage to persons was a more important stimulus to action than did respondents from private institutions.
28. Stimulus to Action: Incident Seriousness
Researchers found that three stimulus to action items were significantly related to seriousness ratings: probability of damage to institutional reputation (p = .045), number of people affected (p < .001), and probability of damage to person (p = .007).

29. Stimulus to Action: Incident Focus
Chi-square tests between stimulus to action variables and incident type showed that all were significantly related at (α = .05) with the exception of “level, status, or rank of person affected.” That is, the importance of a particular stimulus to action was significantly associated with the type of incident being rated with only one exception.

30. Every stimulus to action showed equal to or less seriousness, at a statistically significant level, for data-focused incidents than for people- or systems-focused incidents. There was only one exception to this: “probability of damage/harm to persons.” Indeed for almost every stimulus to action, data incidents had a lower mean score than both people and systems incidents. This seems to indicate that data incidents are substantially different than people or systems incidents.

31. The most frequently recommended foundational best practice for prevention of incidents was education, training and awareness. The second frequently recommended foundational best practice for prevention of incidents was having and following policies and procedures.

32. The most frequently recommended technical best practice for prevention of incidents was patching and debugging systems. The second most frequently recommended technical best practice for preventing incidents was implementing logging, analyzing logs, and monitoring systems. Also frequently recommended were deploying firewalls, IDS/IPS systems, ensuring strong access control systems and passwords, requiring proper configurations, and employing automated quarantining procedures.

33. The two most frequently recommended foundational basic best practice for mitigating the effects of an incident was straightforward communication with affected individuals; this was followed by the establishment and use of interdepartmental communication and collaboration to handle the problem. Also recommended as best practices were decisive and timely action, having and following predetermined and established procedures, and education, training, and awareness.

34. The most frequently recommended technical best practice for mitigating incidents was deploying rapid access control for affected machines. Regular auditing and analysis of logs, deploying automated enforcement tools for standard configurations, and antiviral protections were also felt to be important best practices to mitigate affects.

35. The most highly recommended foundational best practice for managing incidents was having and following pre-established procedures. The second most frequently recommended foundational best practice for managing incidents was having an inter-departmental incident response team already in place.

36. The most highly recommended communications best practices for managing incidents were engaging in frequent and continuous communication with incident handlers, providing communication with the community regarding the incident, and taking quick and decisive action.
VII. Conclusions and Recommendations

A. Observations, Findings, and Things to Ponder

During this study, several very interesting observations have been made. We briefly list and discuss them here, in the hopes of stimulating further discussion among our readers.

1. **There are a lot of incidents happening.** Incidents are happening at a regular pace, with a wide range of targets and scope, and with varied complexity. The CIFAC staff found that literally thousands of additional incidents could have been included in this study because there is no paucity of incidents occurring in colleges and universities. For campuses that keep track of numbers, many lists reflect hundreds or thousands of incidents each semester.

2. **Students are a major factor.** As one might expect, given the population of users examined, the prevalence of students as a major factor is obvious, across all incidents: people-focused, data-focused, and systems-focused incidents. Most campuses have at most four years to teach students about the values, rules, and regulations of the campus before they graduate. During that time, they are experimenting, learning, exploring, and developing their skills and characters. While this period offers opportunity for many accidents and displays of poor judgment, it also provides wonderful learning opportunities and teachable moments for campuses; a time to establish technology related values, ethics, and good practices; a time to learn what risks and responsibilities are incumbent upon the electronic citizen. While students are a major factor in causing the most frequent computer-related incidents, they may not be a factor in the biggest technology-related risks to the campuses.

3. **IT staff members need to talk about these incidents and share information.** We saw the IT professionals on the campuses eager to talk about what is happening and eager to share ideas about what works and what doesn’t. It may be that now, rather than trying to conceal the fact that a computer-related incident has occurred for fear it would reflect poorly on their management or skill, they know that without sharing information about these events, we will not be able solve some of the problems. Without cooperating with each other we will not be able to address the software flaws that are passed on to users with vendor and FOSS software. Without cooperating with each other we will not learn of each others’ practices that reduce vulnerabilities risks. Just as Justice Brandeis argued that the several states are laboratories of public policy experimentation from which the best policies and procedures could be culled and disseminated, so are the thousands of IT departments at colleges and universities a fertile source of new and innovative ideas, information, and solutions.

4. **There is an increase in the use of quarantine zones and procedures on campuses.** CIFAC researchers observed an increase in the use of quarantine zones and procedures to protect campuses from imported viruses and other malicious code. Only a few years ago, during prior research, the notion of quarantining a machine or a set of machines until they could be inoculated and cleaned before reconnecting them to the campus networks was virtually unknown; it would have been considered either technically or practically impossible to do. But now, researchers saw this as common practice on several of the participating campuses. Campuses seem to be maturing in management of information technology and behaviors and practices associated with IT and have been aided in this process by an arsenal of new and relatively simple-to-deploy security technologies.

---

14 The actual quotation is, “It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.” New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).
5. **Interdepartmental incident response teams are increasing.** We observed more campuses with interdepartmental incident response teams than had previously been identified. Earlier in this report we identified a process which was of interest to the research team: the undefining of incidents.\footnote{See page 55 for a detailed explanation of this phenomenon.} The reason given for this was that either too many of those types of incidents were occurring for IT personnel to be able to manage them, or they had been taken off of the radar screen of the IT personnel and passed on as the responsibility of law enforcement officials, university counsel, or other non-IT staff. The CIFAC researchers see a potential danger in this process. It makes sense to have an inter-departmental team and to spread out the work of incident handling among a wider group of responders. However, “undefining” may cause incident data to be lost. The fuller understanding of institutional risk can be compromised when one department simply stops counting incidents through undefining them as incidents. Unless the different departments continuously share information, the institution cannot assess its IT-related risks as a whole and create institution-wide solutions to problems and bad practices.

6. **Having policies, procedures, practices in place prior to incidents is very important.** The CIFAC results show that having policies in place, identifying procedures for handing incidents, knowing with whom to communicate in the event of an incident, having regulations for staff and users regarding the use and management of technology and information, and (perhaps most importantly) following through in implementing these policies is extremely important for prevention of incidents, for mitigating the effects of the incidents, and for managing the incidents. Data also showed that lack of policies and procedures was the cause, and their presence could have prevented many, of the incidents in our sample.

7. **Extensive education and training of users and staff is very important.** The prevention, mitigation, and management of incidents, according to CIFAC participants, could have been enhanced through extensive education and training of users, especially students, IT staff, and non-IT staff. Such training incorporates but is not limited to information regarding policies, standards, institutional values, and awareness of potential problems.

8. **The use of automated response and enforcement tools is important.** CIFAC participants saw the use of technical controls and quarantining of machines as being extremely important. Indeed, the overwhelmingly most frequently recommended technical best practice for mitigating incident effects was deploying rapid access control for affected machines. Also recommended were regular auditing and analysis of logs and deploying automated enforcement tools for standard configurations and for antiviral protections. The most highly recommended best practices for the prevention of incidents were patching and debugging systems, implementing logging systems and analyzing logs, deploying firewalls and IDS/IPS systems, and ensuring strong access control systems.

9. **Risk managers and auditors seem to be absent from the interdepartmental incident handling teams.** The roles of risk managers and auditors appear to not be well understood by IT personnel within the context of computer-related incident and system management. We wonder if the importance, scope, and frequency of computer-related incidents are well understood by risk managers and auditors in relation to overall institutional risk. We were encouraged to see that some colleges and universities did involve personnel in these roles. However, much more is needed if we are to understand and manage institutional and data risks that are associated with computer-related incidents. While we anticipated seeing more data-focused incidents, because we perceive these to be increasing in number and seriousness in the general population, this categorization of incidents did not hold up in our analysis. That is, no cause and prevention factors were primarily related to data-type incidents. We conclude that this fact is more a function of the categorization process than of the occurrence of data related incidents. Risk managers and auditors will play an enormously important role in reducing the risks to data within our institutions regardless of how we categorize such incidents and they must be part of the overall incident assessment and management teams to understand these institutional risks.
B. Five Trends, Conclusions and Recommendations

Executive officers of colleges and universities spend much of their time trying to determine where the scarce resources of their institutions should be spent. They constantly face new requests that vie for their attention, call for expenditure of resources, and claim to be the most critically needed.

The Computer Incident Factor Analysis and Categorization Project has now studied 319 incidents from 36 colleges and universities and collected best practice recommendations for preventing, mitigating, and managing computer-related incidents. Results of analyses repeatedly showed the importance of having policies, training, and automated controls for preventing incidents within these environments. Results showed:

- Having **policies** in place and enforcing them was important in preventing computer-related incidents on campuses.

- Providing **training and education for IT personnel**, requirements for how they perform their jobs and good procedures and practices was important to help them prevent accidental behaviors.

- Providing **training for users** in areas such as security and data protection and more knowledge prior to use of systems was important in preventing incidents.

- Providing more **security awareness** training for users, more stringent user requirement with automated enforcement mechanisms, and better knowledge prior to use of systems was important in preventing careless and accidental incidents.

- Providing more **resources, procedures and requirements** relative to configuration of software and hardware, patching and debugging systems, engaging automated intrusion detection and prevention tools (IDS/IPS and firewalls) and automated compliance tools such as quarantine zones, were important in preventing incidents.

To understand these results, which so strongly recommend policies, requirements, education and training and automated detection and control procedures, the authors recommend the review of five dynamic trends have occurred in recent years.

1. The Move From Centralized to Distributed Systems

Within the last 10-15 years Chief Information Officers, CIOs on many campuses decided, in line with industry trends and the growth of the microcomputer, to place financial resources into the distribution of technology resources, spreading out the services and management of those services to individual colleges and departments. They spent these years building the technology infrastructures of the colleges and establishing fast networks for these communities. For many, this was a liberating process. It allowed access to, and manipulation and use of, data that had been previously highly restricted in controlled data systems.

While liberating to some, this move of data from central repositories to desktops in distributed locations made the job of protecting data not only far more difficult, but perhaps impossible. Data stewards, the individuals who once were charged with ensuring protection of data commensurate with their level of sensitivity, now had to depend on multiple staff members, who reported to other department chiefs and deans, to ensure adequate handling and protection of data. Data protection requirements had to be adequately spelled out in institutional policies so that appropriate procedures could be put into place. The new personnel, having much easier access to stores of institutional data, had to be trained and educated about appropriate data access, transport, and use, procedures. Few institutions were able to develop and execute policies and procedures prior to the technical move to distributed networks. In many cases, those elements have yet to be fully accomplished.
Recommendations:

Ensure that institutional policies and controls are in place regarding appropriate use of campus networks and data and/or bring sensitive data back under control of central systems.

Provide security awareness training for all users in the use of institutional data and establish and enforce appropriate use requirements for staff in the use of networks and in the handling of data.

Ensure that the managers of IT systems are adequately trained to maintain and secure the systems on which institutional data reside or through which they are transported.

2. Fast Changing and Often Inadequately Developed Technology

CIOs are now faced with the trilemma of trying to keep up with the ever-changing technologies on which the campuses have become dependent, keep up with constant demand for upgrades and new software, and do so within shrinking financial resources.

The electronic environments are complex. Nearly everyone on college campuses is using technology for work, social communication, and recreation. Users vary widely in their levels of proficiency in using technology. The ubiquitous nature of networking also makes it possible for other individuals, not necessarily associated with the campus, to connect to campus resources. The fast changing technology requires constant and fast moving education and training of users.

Industry is moving quickly too, rushing products and upgrades to market. In doing so, software that is delivered to the field is often inadequately developed, filled with security holes and operating bugs. When such technology is introduced into a highly networked environment the potential of serious security problems is added. Industry also has continued to produce hardware and software that is designed for use by sophisticated computer administrators. However, the technological skills of the increasingly diverse population of computer users vary tremendously. In many cases, the technology user interfaces are complicated and lack transparency. By placing increasingly sophisticated hardware and software into the hands of a diverse and under-trained population of users, security vulnerabilities are added and the communities, their systems and their data are put at risk.

Information technology personnel, those charged with managing these environments, find themselves in a perpetual state of stress and uncertainty. They are responsible for trying to keep up with identifying and applying security patches for flawed software products. They are expected to satisfy and serve a growing body of diverse users. They are responsible for learning about, and managing, new hardware and the interoperability of different operating systems and platforms. And, as the CIFAC study has shown, they are trying to manage the increasing number of computer-related incidents that are occurring.

Recommendations:

Ensure that vulnerability scanning is done for all systems on campus and that IDS/IPS tools are used when appropriate.

Work with other institutions to collaboratively communicate to vendors the user-interface requirements, the need for transparency, and the need for more fully developed and tested products, employing the collective market power of the higher education community to encourage vendors (including the FOSS community) to create more secure and usable products.

Ensure that institutional requirements are in place and enforced, spelling out the procedures that must be taken in managing systems connected to the campus networks.
3. Resistance to Training and Education for System Administrators

CIOs know the value of training and education in institutions of higher education. However, it may be the case that education is spoken about so often that it is taken for granted or its importance minimized as the new, more intriguing products are introduced by vendors. Creating policies, establishing requirements for users, and providing training for the IT staff who manage the technology may seem to be mundane tasks that can be put off until the pressure for putting technology into place is lessened – until the users are “up and operating.” However, the CIFAC results indicate that this cannot be the case any longer. Policies, education, and training need to be placed at the top of resource priorities. Policies, user training, configuration requirements, and clear expectations for technology use, need to be recognized as critically important elements in reducing enterprise risks and saving resources in the long term.

There has also been a hesitancy, or perhaps even resistance, in many colleges and universities to provide skill training and education for systems administrators. Establishing a career path for information technology personnel and thereby pairing skill levels with specific work assignments creates two dilemmas for management.

The first has to do with availability of skilled IT personnel. If managers specify the level of skill required to perform specified tasks, then they have to fill those positions with individuals who possess that level of skill. The shortage of available information technology personnel has led some administrators to place unprepared staff members and students into a system administrator capacity. Additionally, because powerful hardware has been introduced into the market at relatively low prices, individuals without adequate skill and training are able to purchase such equipment, and without adequate network controls, attach it to campus networks and manage (and frequently mismanage) it themselves.

The second dilemma created by establishing a career path for IT personnel has to do with retention and the market demand. If an appropriate skill and responsibility related career path is created for IT personnel, and no individuals can be found to fulfill the escalating levels of required skill, then training needs to be provided or purchased. At the present time, the quality of private certification and training programs for system administrators varies widely. College and university IT managers who provide training for system administrators or who pay for them to receive such training know that once training is received, the market value of that employee increases. Often, with additional training, the employee is more marketable and is hired away from the academic environments to corporate settings where salaries are higher. This may cause employees to leave after gaining certification; on the other hand, it may reduce turnover and increase loyalty. The relative benefits and costs of such an advancement program need to be considered on a institution-by-institution basis considering more variables than can be discussed here.

The CIFAC study results have shown that having policies in place and following them is the most important element in preventing computer-related incidents. Training and education for IT managers and staff, for non-IT staff, standards, training, and awareness for faculty and for students, was found to be very to extremely important for preventing incidents. Lack of policies and training and education was found to be a cause of more than half of the incidents reported. However, if providing training means that personnel resources are lost, there may be resistance to formalizing such training. This will be detrimental to enterprise risk management.

Recommendations:

Ensure that institutional policies and controls are in place regarding appropriate use of campus networks and data.

Ensure that institutional policies and required procedures for managing resources are known by all IT personnel and enforced.

Provide training and education for all systems and network managers commensurate with the skill levels required to appropriately manage the campus systems and networks.
4. Short Window of Opportunity for Training Users

It might be easier to place the blame for computer-related incidents on external, unauthorized and malicious individuals. However, this study has shown that to be an error. Accidental or careless behaviors of staff and students were the causes of nearly 40% of the incidents reported. Many of these behaviors were felt to be the result of lack of awareness and knowledge, absence of policies, and the lack of training regarding requirements, policies, and technology. However, in institutions of higher education, the window of opportunity for training users is short and the population of users is constantly changing.

Where should executive officers and managers place their resources when there is such a short window of opportunity for such a rotating population? In academic settings, researchers recommend, and the CIFAC data support, that having policies in place, having clear regulations and requirements for the use of campus common resources, and having adequate and on-going security awareness training for users are the most important efforts to undertake. CIFAC respondents highlighted the importance of requirements and enforcements for those requirements and spoke at length about automated enforcement of configuration requirements. These were identified as important in getting out the message to the community about what was important in using the technology, about why it was important, and about their obligations in a shared resource environment.

Even though the technology continues to be built for more sophisticated systems managers, and though the user population is continually growing in technological sophistication, the CIFAC results point to awareness training and campus requirements, rather than in-depth operating system or software training for users, as the primary effort to be undertaken. What seemed to be missing and a cause of computer-related incidents was basic requirements, enforcements of policies, awareness of rules and best security practices, and general technology education for campus users while they are in the short training window. What was lacking was not instruction about specific applications, but rather a deeper understanding of computing ethics and the communal management of a common pool resource.

Recommendations:

Provide security awareness training for all users regarding their personal information, regarding campus shared resources, and regarding their responsibilities within a networked shared electronic environment.

Ensure that campus appropriate use requirements are known by all users, that the rationale for these requirements is known and understood, and that the requirements are enforced.

5. Responsibility on the Shoulders of IT Personnel

As systems and data became more distributed, as the community increased its dependency on computers, and as the user community became more diverse in skill, the primary responsibility for procurement, installation, operations, maintenance, and security of IT systems squarely placed on the shoulders of IT personnel. Systems administrators were expected to become expert in the management of multiple operating systems and network protocols. They were held responsible for unauthorized data access, for external breaches of security, for system crashes, and other negative events, while seldom receiving praise for their successes. This is still the case in many colleges and universities. This expectation of responsibility often existed without a clear understanding about who had the authority to manage the systems. Responsibility without authority makes for an untenable position.

As computer-related incidents continued to increase, and many drew attention from the popular press, system administrators seemed to take, or were given, more control and authority to manage the networks. They also recognized that they could not take all of this responsibility themselves. A wider institutional perspective was required for the management of the incidents. A more interdepartmental approach would enhance the investigation and handling of computer-related incidents.
It is important that college and university administrators remember that IT security, like any type of security, is a negative deliverable: computers and networks are expected to be operational at all times, and they are only noticed when there is a problem. Just as police departments are praised when crime rates decline, so should advances by IT departments be properly recognized and rewarded by administrators. Providing reliable, high-quality IT resources is not like turning on a light switch; it requires meticulous planning, constant monitoring, and a continual process of trial and error to develop the best services possible. It is easy to complain about occasional IT problems, but the demoralization of IT staff that this causes does a disservice to the community. Blame should not be the only thing placed on the shoulders of IT staff; credit should also be given where it is due.

The CIFAC data show that interdepartmental incident response teams are increasingly being used on campuses. They are recommended as best practices for mitigating and managing the incidents. The data show that network controls such as quarantine zones are being used, evidence that IT personnel are taking more control of the computing shared environments. Automated detection and prevention systems, firewalls, and quarantine zones were among the most strongly recommended best practices for preventing and mitigating effects of computer-related incidents. There is evidence that system administrators are collaborating in the investigation, handling, and resolution of computer-related incidents. There is evidence that colleges and universities are more appropriately distributing the responsibility for their electronic environments and clarifying the authority for the management of such environments. The high level of cooperation shown to the researchers in the CIFAC study, contrary to self-protective secretiveness that could be the case, is evidence that colleges and universities are eager to learn from each other and to share their wisdom regarding computer environments and incidents.

**Recommendations:**

Ensure that responsibilities and authority are aligned for IT and non-IT personnel in the management of networks and institutional data.

Authorize and ensure that automated procedures are utilized to improve on incident detection, prevention, and response.

Encourage the establishment of interdepartmental teams for incident response and management.

Ensure open and rapid communication with the campus community when an incident occurs and regarding its resolution and management.

Involve campus auditors and risk managers in the discussions regarding computer-related incidents to enhance enterprise-wide risk management and the prevention of incidents.

Learn from others by sharing information about incidents and best practices for prevention, mitigation, and management.

Establish systems to reward successes by information technology staff and managers.
VIII. Reflections and Next Steps

Researchers began this project to determine if a common language could be established to help IT professionals share information about computer-related incidents, and to see if factors that are related to the occurrence of computer-related incidents could be identified.

A. Regarding a Common Language

We introduced a categorization system that asked participants to identify incidents by their focus (people-focused, data-focused, and systems-focused). During data collection we not infrequently observed respondents having difficulty with that system. At times it appeared that they were trying to select from multiple categories for a particular incident. Perhaps the incident had data, systems and people components. Or, perhaps the incident changed over the course of its event (for instance, starting out as a prank against a person, but then finding data that was economically valuable and becoming a data theft incident). Some incidents are very complex and can have multiple foci, and a single incident may take a long and winding road between inception and conclusion.

Most frequently, we saw participants seeming to choose between categorizing the incident based on what they thought the perpetrator’s focus was and their own perception of what it would take to fix the incident. For instance, in the judgment of a respondent, the perpetrator of an incident may have been after data, and therefore the respondent categorized the incident as data-focused. However, they would have to take immediate action on the system to respond to the incident and therefore the incident could be categorized as a system incident. This kind of vacillation and potential confusion raises questions as to the usefulness and validity of the categorization scheme.

Some people have suggested that all incidents are, in truth, data incidents. That is, regardless of who the perpetrator or actor is, and regardless of the system on which it takes place, data are involved. Computers are, at their root, merely data crunching devices, and networks are merely a data transport mechanism between computers. Others have suggested that all incidents are, in truth, people incidents. That is, regardless of what system is involved, and regardless of what the specific data were that were released, altered, stolen or accessed, some person(s) was responsible for the error or the action. What’s more, an incident is only an incident when a person is affected; to paraphrase the popular question, if a packet drops in the ether and nobody notices it, is it an incident? And there are those who would suggest that all incidents are, in truth, systems incidents. That is, it doesn’t matter what person is involved, or what data is targeted, it is happening over a system and there could be system safeguards or fixes put in place to respond to it. By definition, this theory argues, a computer-related incident must involve a computer – a system.

The CIFAC data seem to indicate that the terms “people-focused incidents” and “systems-focused” incidents do have some meaning to our respondents. With only one exception (level, status, or rank of people affected), the importance that each of our respondents placed on each of the stimulus to action variables was significantly related the type of incident it was. People- and systems-focused incidents were much more important to our respondents than were data-focused incidents.

Does this categorization system hold any promise for use in the field?

To the degree that categorizing incidents helps respondents focus their efforts and identify the relevant stimuli to action more quickly, we think that it has some benefit. In this regard then, we argue that this categorization activity may be helpful in objectively determining the seriousness of an incident, providing a paradigm through which to view the incident, and suggesting starting points in mitigating the incident’s effects and managing its resolution. Certainly, more clarity must be achieved when asking respondents to categorize incidents, which requires that the terms “data,” “people,” and “systems” are universally understood in essentially the same way – a semiotic question of deep import but no ready solution. Because we cannot guess the motivation of an
incident perpetrator, if indeed there is one, incident responders must stay focused on the variables of seriousness, and how quickly we need to respond.

B. Regarding Factors Associated with the Occurrence of Incidents

The analysis of data from the cause and prevention questions within the CIFAC study has shown that four factors are associated with cause and prevention of computer-related incidents. Three of the factors have to do with people and one with networks:

- For the factor that is related to IT personnel, it appears that more education and training, more requirements as to how they perform their jobs, and procedures that help prevent them from accidental or careless behaviors are important in preventing incidents.
- For the factor that is related to users, it appears that more education and awareness training, more or more stringent, requirements, and better knowledge prior to use of systems, would be helpful in preventing them from the accidental or careless behaviors that cause incidents.
- For the factor that is related to networks, more resources, procedures, and requirements relative to configuration of software and hardware, would be helpful in preventing incidents.
- For the factor related to non-IT staff, more education, stricter or more requirements, and more knowledge prior to use of systems would help to prevent the accidental behaviors that are the cause of incidents.

It is interesting to note that the CIFAC study conclusions circle back to where the CIFAC study focus group participants first pointed. Results from the focus groups revealed that “user education or lack thereof” was identified most frequently as a causative factor for the incidents. “Poor or non-existent policy” was the second most frequently identified cause of computer-related incidents. “Too much or inappropriate access” and “lack of physical security” – perhaps also reflecting poor or non-existent institutional policy or insufficient user education – were identified as very important causes of incidents.

Are there specific factors associated with the occurrence of computer-related incidents?

Yes. Four factors were identified. Three have to do with people (IT personnel, non-IT staff, and academic users) and one with networks. Having and following policies, implementing and enforcing them, and providing education and training about technology use and standards are important for the prevention of computer-related incidents.
Appendices

A - Literature Reviews

B - CIFAC Instrument

C - Participating Colleges and Universities

D - Sample of CIFAC Incidents

E - Statistical Analysis

F - Best Practice Scoring Scales

G - Rationales For Ratings by CIOs
Appendix A: Literature Reviews

Literature Review Relative to Terms and Definitions

Definition of Incident: Agreement on need for common language
Throughout the literature on incidents and incident response, there is surprisingly little agreement on what an incident is; this has been noted by many authors, including recently by Killcrece et al. (2003). Many authors bypass the issue altogether, implicitly relying on individuals and colleges and universities to make their own assessments as to what constitutes an incident. In practice, the definition of incident is often the same as Justice Stewart’s now-famous definition of obscenity: “I know it when I see it.”

Lucas and Moeller (2004) acknowledge the import of the institutional establishment of a definition of an incident a priori the occurrence of one. They write:

[T]he type of activity that is considered to be an incident should be clearly decided up front. It is strongly recommended that a clear, concise definition be developed for the ‘incidents’ a team will address. Generic or vague definitions such as ‘unauthorized activity’ leave too much room for interpretation and may negatively affect operations. For example, the number of personnel assigned to the team may prove insufficient for the volume of ‘unauthorized’ activity reported and problems may be encountered in trying to enter and track the incident data in a database of trouble ticket system.

In other words, an imprecise or overly broad definition of an incident allows policy writers and response teams to slide into a postmodern morass where everything is simultaneously both an incident and not an incident. Lucas and Moeller, like most practitioners, agree on the need for a precise definition that provides a rigorous rule for clearly differentiating “incident” from “non-incident.” Although this has not been discussed in the literature, the corollary of Lucas and Moeller’s injunction to define on an organizational level is that the process of defining what an incident is as an organization provides a heuristic tool for determining the very purpose of an IT group in and of itself and also within the larger organizational milieu.

The Network Working Group of TERENA, the Trans-European Research and Education Networking Association, a kind of meta-network of higher education IT groups, published RFC 3067 in February 2001. This document, entitled “Incident Object Description and Exchange Format Requirements,” is intended “to establish cooperation and information exchange between leading/advanced CSIRTs (computer security incident response teams) in Europe and among the FIRST community.” Recognizing the importance of a “common language,” they state:

Computer Incidents are becoming distributed and International [sic] and involve many CSIRTs across borders, languages, and cultures. Post-Incident information and statistics exchange is important for future Incident prevention and Internet security improvement. The key element for information exchange in all these cases is a common format for Incident (Object) description.

Nancy and Peter Finn were among the first to research computer-related incidents, although they viewed and defined them strictly from a legal framework. In a 1984 article in Computerworld, they paid specific attention to the growing threat of computer crime. The Finns divided computer crime into five categories: financial crime, information crime, theft of property, theft of services, and vandalism. However, they paid no attention to

---

the accidental or non-malicious aspects of IT-related incidents and chose to focus on crime-specific threats. Interestingly, Nancy and Peter Finn were a computer consultant and an attorney, respectively, making their article one of the first explorations of computer incidents from an interdepartmental standpoint.

One fundamental question in defining incident is whether the word “incident” is atomic in nature or whether it represents a collection of otherwise discrete occurrences. Howard and Longstaff (1998), in their groundbreaking work on incident taxonomies, define an incident as “a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing.”21 An attack is the atomic element, defined as “a series of steps taken by an attacker to achieve an unauthorized result.” An attacker is, in turn, “an individual who attempts one or more attacks in order to achieve an objective.” These definitions are similar to the ones employed in Howard (1997).22 TERENA (2001) defines an attack similarly, although in a more verbose form, as “an assault on system security that derives from an intelligent threat… to evade security services and violate the security policy of a system. Attack can be active or passive, by insider or by outsider, or via attack mediator.”

While this definition marks a major advancement in the definition of incidents, we feel that it suffers from several problems. First, attack and attacker are defined tautologically. Second, and more importantly, the use of the word “attack” to describe a single event implies malicious intent upon the part of the “attacker.” Many incidents, including many used in our focus group instruments, lack intent to violate rules or norms, much less any malicious intent to do so. Indeed, a sizeable proportion of incidents are undoubtedly pranks or jokes with unintended detrimental ramifications; more still are simply the result of accidents or actions undertaken without seeing any negative consequences. The word “attack” implies an intentional assault against a system. This unnecessarily focuses attention on security-related events and malicious attacks on people and their data, which compromise just a portion of total incidents.

Grance, Kent, and Kim (2004),23 like Lucas and Moeller (2001), stress the need for a clear institutional definition of what an incident is. Indeed, they consider this to be the first step in creating an effective incident response team – without such a definition, how will the team know what to respond to? They further define an “event” as “any observable occurrence in a system or network” and “adverse events” as “events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a Web page, and execution of malicious code that destroys data.” Rhetorically, this creates an important but subtle distinction: it establishes those occurrences which cause any effects as “events” but adds an adjective to designate those which cause specifically negative effects. Under this definition, if n packets are required to crash a website, the first n-1 packets cause “events,” but packet n causes an “adverse event.” Many of the things that cause incidents or attacks are not detrimental in and of themselves, but become detrimental only in a specific context. Grance et al. make this distinction in ways that other authors have not.

Grance et al. focus on computer security events in particular; they use the terms “incident” and “computer security incident” interchangeably. They admit that the definition has evolved and discuss the expansion of this definition. They give the examples of denial of service, malicious code, unauthorized access, or inappropriate usage, but stop short of offering a final definition.

Similarly, Van Wyk and Forno (2001) rely primarily on examples of incidents. They do include a basic definition, though: “In the most basic terms, an incident is a situation in which an entity’s information is at risk, whether the situation is real or simply perceived” [emphasis added].24 Van Wyk and Forno represent a more holistic school of thought on incidents. They look beyond security incidents to a definition that is more inclusive of other organizational threats, such as the potential loss of data or the exposure of confidential data.

Significantly, they expand the definition to include situations that might include false alarms. This is an important part of the definition; if only “real” incidents attracted the attention of incident response teams, this would mean by definition that damage or exposure would have to occur before involvement. It would be as if fire fighters would only respond to calls after callers could produce verifiable evidence of fire damage. That Van Wyk and Forno include perceived incidents means that incident response teams can take a more proactive approach to the staunching of incidents before their detriment is manifested.

TERENA (2001, section 2.2.7) defines an incident in very extensive terms:

An Incident is a security event that involves a security violation. An incident can be defined as a single attack or a group of attacks that can be distinguished from other attacks by the method of attack, identity of attackers, victims, sites, objectives or timing, etc.

[…]

However we should distinguish between the generic definition of ‘Incident’ which is an event that might lead to damage or damage which is not too serious, and ‘Security Incident’ and ‘IT Security Incident’ which are defined below:

a) Security incident is an event that involves a security violation. This may be an event that violates a security policy, UAP, laws and jurisdictions, etc. A security incident may also be an incident that has been escalated to a security incident.

A security incident is worse than an incident as it affects the security of or in the organisation. A security incident may be logical, physical or organisational, for example a computer intrusion, loss of secrecy, information theft, fire or an alarm that doesn’t work properly. A security incident may be caused on purpose or by accident. The latter may be if somebody forgets to lock a door or forgets to activate an access list in a router.

b) An IT security incident is defined… as any real or suspected adverse event in relation to the security of a computer or computer network. Typical security incidents within the IT area are: a computer intrusion, a denial-of-service attack, information theft or data manipulation, etc.

As with many other research documents, this TERENA RFC focuses on the security incident as the primary focus of incident responders; other incidents are essentially ignored. However, the definition remains so broad that virtually anything could be considered a security incident. Like Van Wyk and Forno (2001), TERENA gives a nod to suspected incidents as being as important as actual incidents.

FedCIRC, the U.S. federal government group under the Analysis and Infrastructure Protection (IAIP) Directorate of the Department of Homeland Security (DHS) tasked with incident reporting, defines an incident in loose terms, as follows:

An incident is the act of violating an explicit or implied security policy. Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations.

These include but are not limited to:
- attempts (either failed or successful) to gain unauthorized access to a system or its data,
- unwanted disruption or denial of service,
- unauthorized use of a system for the processing or storage of data, and,
- changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction, or consent.

---

Again, an incident is described solely in terms of security. (This is also the case in Information Technology – Code of practice for information security management, better known as ISO 17799.\textsuperscript{26}) Under this definition, accidentally placing the unencrypted Social Security numbers of all of the Department of Homeland Security’s employees on the DHS’s home page would not qualify as an incident. Notably, though, FedCIRC considers failed unauthorized access attempts as incidents, showing a proactive attitude. Many other definitions would reduce failed attempts to the non-incident category.

CIFAC’s parent project, ICAMP, defined an incident as “any event that takes place through, on, or constituting information technology resources that requires a staff member or administrator to investigate and/or take action to reestablish, maintain, or protect the resources, services, or data of the community or individual members of the community.”\textsuperscript{27}

In the CIFAC/EDUCAUSE workshops, we defined incident in the following way and collected responses from our focus group participants:

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 owner(s) and/or administrator(s) of the IT systems in question,
- Violates norms commonly accepted within the community of system user(s) of the system(s) in question for use of IT resources,
- AND/OR the attempt or conspiracy to engage or represent oneself or another to be engaged in or actively planning to engage in any aforementioned behavior.\textsuperscript{28}

While the overall reaction to our definition was positive, many participants commented that it read like “legalese” and was too unwieldy for practical use by incident response personnel. In retrospect, we completely agree.

**Undefining**

During this project we identified a phenomenon which we call “undefining of incidents.” Many events that were previously considered to be computer incidents within colleges/universities are now, due to more clearly defined roles and responsibilities for IT personnel, more rapidly being undefined and handed off to other organizational divisions. They are being undefined as computer-related incidents because they no longer fall within the perceived radar scope of information technology staff members. Undefining also appears when the number of occurrences of a particular type of incident is so great that such incidents can no longer be economically recorded and managed by the incident response team or the current incident tracking software. Common examples of this include illegal file sharing and excessive bandwidth use incidents. Those incidents, previously labeled by some as copyright violations or illegal file sharing, are being undefined as computer-related incidents and handled, in bulk, either by technical system modifications or, in some cases, the throwing up of hands and assumption that the university counsel, student affairs staff, or another division of the college or university will deal with them.

It is important to delineate roles and responsibilities to accomplish efficiency in work effort. However, too rapid a handoff, too complete a partitioning of incident handling responsibilities, or the undefining of incidents may render it impossible to track incidents from notification to resolution. This, in turn, makes it difficult to evaluate the effectiveness of incident management, share and compare information and best practices across


institutions, and thoroughly understand the kinds of technical, educational, and/or policy interventions that are needed. If the incident involves information technology, we need to ensure that we are aggregating information in such a way that any technical changes that are required, regardless of whether the incident was deemed a student affairs matter, a legal matter, a policy matter, are evaluated and implemented. To accomplish this, there is agreement that we need a common set of definitions and a common language for discussing incidents.

Conclusions Regarding Definition
We are hesitant to bring yet one more set of definitions to the discussion, in the face of the already existing confusion in terms that exists in the literature. However, like Killcrece et al. (2003), we strongly support the need for definition and consistent use of terminology in the field of information technology. Like Grance et al. (2004), we conclude that clarity and understanding of what a computer-related incident is has evolved over time and with increased experience. In the vein of the work by Van Wyk and Forno (2001) and information gathered informally through extensive discussions with active security professionals, we conclude that the scope of threat to the college or university as a whole, as well as the institutional mission, must be recognized and carefully considered as “computer-related incident” is defined. Any such definition must also include risks to electronically-stored data, including corruption, falsification, theft, and improper dissemination; such a definition must transcend technical security measures and be cognizant of the damage that non-security incidents can cause.

Our primary obligation in this attempt to define computer-related incidents is to institutions of higher education. Our conclusion is that efforts which narrowly define incidents as security-related such as in the aforementioned definitional literature authored by FedCIRC and TERENA are too restricting and can leave responders unnecessarily myopic as they search for best practices and the most effective responses to computer-related incidents. We, like Grance et al. (2004), recommend that each college/university clarify its terminology prior to managing incidents and set specific tolerance and response thresholds for particular types of incidents. Still, a common set of basic terms must be adopted across colleges and universities if we are to learn from each other.

The CIFAC staff, at this time, recommends the following definition. It is indebted to the work of Grance et al. (2004, p. 2-1.), who write that “an incident can be thought of as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” Our work incorporates our own experience, comments from professionals in workshops and personal interviews, and commentary from the literature reviewed in this report. Please note that we expect to test and perhaps further refine this definition over the course of the next 18 months during the NSF-sponsored CIFAC study, and that it is by no means set in stone.

Computer Incident—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.

Literature Review Relative to the Organization of Computer-Related Incidents

Taxonomies and Categorizations: Organizing incidents
The concepts of “taxonomy” and “categorization” are, despite their frequent use as synonyms, inherently different ideas. They differ in terms of type of organization and the narrowness of their focus; in practice, in whether they focus entirely on technical vulnerabilities, or on the larger realms of incidents and security events. This distinction is particularly relevant to the CIFAC study, as we seek to look at the full range of computer-related incidents.

Taxonomies
The definition of “taxonomy” may seem evident, but the word is used with several different meanings within the literature. For this reason, some discussion of definition seems constructive. Generally speaking, taxonomies create logical structures based on a tree-and-branch system where one feature is dependent upon its parent. Outside of the IT world, the Linnaean taxonomy of life is perhaps the best known taxonomy; every life-form
within a taxonomical level (kingdom, phylum, class, etc.) shares certain salient features with those below it, but usually not parallel to it, and life-forms below it are further split depending on their characteristics. The important thing to note here is that taxonomies are strictly hierarchical; there is no overlap of sub-category. Humans and chimpanzees are both in the order “primates,” but have different families, genus, and species. Each category breaks off into one or more sub-categories, but a sub-category can only be a member of one category. That is, all members of genus Homo are in family Homonidae; a sub-category can only have one category. In a sense, taxonomies provide nominal and ordinal organization to the items they include.

Because there are no characteristics of an IT incident that are inherently a priori other characteristics, taxonomies quickly fall flat when used by practitioners working in a time-sensitive situation. An analogue to taxonomies of IT incidents would perhaps be creating one for sports balls. If we have a baseball, an American football, a soccer ball, and a cricket ball, how do we taxonomically categorize these? Do we start with size (baseballs and cricket balls are small, footballs and soccer balls are large)? Or do we start with shape (cricket balls, baseballs, and soccer balls are round, footballs are oblong)? Or do we start with a defining characteristic of the sport it is used in (in baseball and cricket, players hit the ball with a bat, while in soccer and football external implements creating torque are expressly prohibited)? As none of these categories exists a priori the others, putting balls into a taxonomical structure is a difficult exercise.

Howard (1997) argues that “taxonomies should have classification categories with the following characteristics”: mutual exclusivity, exhaustiveness, unambiguity, repeatability, acceptability, usefulness. His work at creating the taxonomy is tempered by this warning:

[A] fundamental problem is that, assuming an exhaustive list [of incidents] could be developed the taxonomy would be unmanageably long and difficult to apply. It would also not indicate any relationship between different types of attacks. As stated by Cohen, ‘… a complete list of the things that can go wrong with information systems is impossible to create…. [T]here are a potentially infinite number of lists that can be encountered, so any list can serve only a limited purpose.’

Howard points out that these problems apply to results categories, empirical lists, matrices, and other taxonomical systems as well. There seems to be, in Howard’s mind, a tradeoff between the completeness of the taxonomy of incidents and the usefulness of that taxonomy to practitioners. Howard establishes a taxonomic organization of incidents that, while of questionable use to incident responders, does provide a fascinating and well-developed rubric for security researchers. Fundamentally, taxonomies seem to be of most use to researchers, but their extensive and detailed nature means that they are of less use to those trying to respond to an incident with all due urgency. To go back to the example of the Linnaean taxonomy, it is far easier to point out, given limited time, that humans have a skeletal system, opposable thumbs, and an endothermic circulatory system than it is to go through the full Linnaean taxonomy to inductively describe physical characteristics. However, the Linnaean taxonomy is the standard within the biological sciences, and few researchers would advocate its abolition in favor of simply stringing together appropriate but vague adjectives.

While Howard’s research is probably the most significant to the field (he is cited by virtually everyone working on taxonomy issues), TERENA’s RFC 3067 (2001), is significant to other research on inter-institutional taxonomical definition and information sharing. It is not a document for practitioners of incident response, but a definition of “a common data format for the description, archiving and exchange of information about incidents” between CSIRTs....” It primarily deals with the nitty-gritty technical details on incident information exchange (what information should be collected, how it should be organized, the formatting of dates and IP addresses, etc.) rather than creating a rigorous taxonomical framework with which to view and categorize incidents.

In addition, Aslam, Krsul, and Spafford (1996) provide a security fault classification system for UNIX computers. It is, by its own admission, a classification system, despite being called a taxonomy in the article title. It provides an interesting rubric with which to consider the specific operating system-based vulnerabilities

of one particular operating system. Schultz and Shumway (2002) provide a rigorous classification scheme as well, but call it a taxonomy as well. Like so many other words in the field, it seems that “taxonomy” is very ill-defined.

Landwehr et al. (1994) focus narrowly on program security flaws. Their work is based on the taxonomical assignment of recorded incidents, so rather than attempting to fit empirical evidence into a model, they construct a model around existing data. Their definition of taxonomy is particularly noteworthy:

A taxonomy is not simply a neutral structure for categorizing specimens. It implicitly embodies a theory of the universe from which these specimens are drawn. It defines what data are to be recorded and how like and unlike specimens are to be distinguished. In creating a taxonomy of computer program security flaws, we are in this way creating a theory of such flaws, and if we seek answers to particular questions from a collection of flaw instances, we must organize the taxonomy accordingly.  

Practitioners in the field have made it clear that computer-related incidents are dynamic events. They may represent a single human act or a series of acts. Even single acts may set off a series of technical happenings. Often a single human act becomes a series of actions as the person finds new vulnerabilities or “opportunities” to exploit, as technical defenses are activated, or as IT staff members respond to the initial behaviors; the intruder-administrator cat-and-mouse phenomenon is well-known and well-documented. For this reason it seems particularly difficult to organize computer incidents themselves into taxonomies.

While technical researchers and those directly responsible for eliminating specific system vulnerabilities may find taxonomies of vulnerabilities of great value, a broader view of incidents and categorization of such seems of more usefulness to those trying to quickly determine the seriousness of the incident and the best approach for managing it. Categorization systems best help deliver the “big picture.” This appears to be what non-technical personnel with an interest in information technology security and continuity need to make appropriate decisions regarding incident prevention and management.

Intermezzo: Lists

The obverse of the taxonomy is the simple listing—a naming or nominal organization. The Common Vulnerabilities and Exposures (CVE) listing by MITRE makes much of the fact that it is “a dictionary, not a database.” The CVE is a listing of all vulnerabilities and exposures that have been catalogued and enumerated (in the format CVE-year-xxxx) by the CVE team. They have their own problems with defining vulnerability and exposure, but have settled on a definition. It reads in short form:

In an attempt to remain independent of the multiple perspectives of what a “vulnerability” is, the CVE identifies both “universal vulnerabilities” (i.e. those problems that are normally regarded as vulnerabilities within the context of all reasonable security policies) and “exposures” (i.e. problems that are only violations of some reasonable security policies).  

A longer form of these terms appears on MITRE’s CVE web site.

The main problem with the CVE work is that the information is at a general level and does not help managers know specifically how to determine if any given vulnerability exists on any given system(s). A new assessment language called OVAL has been created by MITRE to help make the vulnerability alerts more useful to

---


33 This is available online at <http://cve.mitre.org/about/terminology.html#Def2>.
individual sites and organizations.\textsuperscript{34} Again, this is valuable work, being especially beneficial for the specific investigation of vulnerabilities by site, but it does not address the broader range of incident causes and effects.

For many years, authors have been producing and managing lists that identify known threats and vulnerabilities in operating and networking systems. The SANS Institute regularly issues updates to its list, entitled “How to Eliminate the Ten Most Critical Internet Security Threats.”\textsuperscript{35} To assist system administrators in knowing which vulnerabilities to address when resources and time are limited, the Institute, working with a large group of security experts, identifies the top ten vulnerabilities and provides information about how to respond. A list provided formerly by the Silent Runner group, a division of Raytheon which has since been absorbed by Computer Associates, is similar in nature. This list is, unfortunately, no longer published. Lists such as these provide incident handlers and managers with valuable, albeit narrow, system and network-focused information.

Some publications specialize in providing information about particular types of threats such as viruses. \textit{The Virus Bulletin}, for instance, provides up-to-date and detailed information about new and old viruses as well as information about tools to help administrators protect against viruses on their systems. Known for its outstanding work in analyzing new viruses and communicating the new threats that such contain, this organization is purposefully narrow in focus.\textsuperscript{36}

Review of incident documents in several colleges and universities, shows another kind of incident listing. Many schools have created such lists, which help IT groups organize incidents by type. They do not necessarily imply any relationship between types or hierarchy of severity/importance. 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.

The reorganization of lists into more categorical units, as we have seen in other college and university incident-type lists, is important to study further. It seems to show the efforts that college and university personnel are taking to make sense of the relationships between different incident types and to gain perspective on the causes of incidents, the severity of incidents, and appropriate corrective response. Only a few colleges and universities have begun to categorize or codify computer-related incidents and establish thresholds to trigger appropriate responses. Thresholds might include the number of systems or people affected, a particular level of financial damage, employee repair time required, etc.; responses occur when these thresholds are met or exceeded. Responses might involve certain actions being taken automatically to correct damage or prevent further damage, as well as the automatic involvement of certain members of the college or university community. However, such codified and automatic response seems to be the desired goal of many and marks an important advance in incident management. Most higher education IT groups lack the time and funding to complete such a mammoth task. In addition, if each IT department creates their own categorization schemes, it not only impedes inter-institutional sharing, but causes EDUCAUSE’s members to reinvent the wheel 1900 times. Therefore, it makes more sense for this important work to be done on the inter-organizational level through consensus and cooperation.

It has been suggested that information sharing and analysis centers, better known as ISACs, might take the lead on categorization and threshold-creation. These organizations were suggested by Presidential Decision Directive 63, issued by President Clinton in 1998, as a “mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies.”\textsuperscript{37} There are now over two dozen American ISACs representing various areas of the national critical infrastructure. Unfortunately, due to their exclusive membership of large for-profit corporations, the two ISACs of most interest to those studying information security, the IT ISAC\textsuperscript{38} and the Financial Services ISAC,\textsuperscript{39} hold their cards very close to their chest. We were

\textsuperscript{34} For more information on OVAL, see <http://oval.mitre.org/>.
\textsuperscript{35} This is available online at <http://www.sans.org/top20/top10.php>.
\textsuperscript{36} The Virus Bulletin is published at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, UK.
\textsuperscript{38} For more information on the IT-ISAC, please see <https://www.it-isac.org/>.
\textsuperscript{39} For more information on the Financial Services ISAC, please see <http://www.fsisac.com/>.
unable to successfully gather any significant information about the way in which ISACs categorize or share information about incidents. Professionals in the field, however, generally believe that the ISACs are still some time from doing any meaningful work in incident categorization or analysis.

The most applicable ISAC to the college and university community is the Research and Education Network ISAC, or REN-ISAC.\(^{40}\) This organization, based out of Indiana University at Bloomington, acts as an information aggregation and dissemination nucleus for member higher education institutions. It receives, analyzes, and disseminates network security operational, threat, warning, and attack information within higher education. It provides a conduit for information to colleges and universities regarding aggregated data on specific security related multi-organizational incidents and measures rates of increase or decrease in activity related to the event. At the present time, most of the information regarding these security incidents is coming from net-flow logs. REN-ISAC is helping colleges and universities manage and respond to these incidents. While there is a desire to categorize incidents, determine thresholds for response, and define such elements as severity, these definitions and categorizations have not yet been accomplished.

For all of the IT-related ISACs there are questions related to the adequacy and future use of the data. Questions include: who will actually report, and to whom, what will be the qualities and quantity of information reported, what types of information will be included, how complete will the information be, and what will happen with the information once reported. It is too early to determine whether the IT-related ISACs will become major assists to colleges and universities in the management of computer-related incidents.

Categorization

Related to the notion of the listing is the idea of a categorization, what CIFAC is attempting to establish. Indeed, much of the extant categorization literature self-describes as taxonomical, even when it appears, using Landwehr’s definition (1994), to be categorical. Using standard dictionary definitions and Landwehr’s insight, there is indeed a clear difference, although in practice it has been blurred. Therefore, categorization work has been largely discussed with taxonomies above, as well as in the section discussing the definition of incident (e.g.: Finn and Finn, 1984). Making a distinction for our purposes is important, but trying to divide previous work is dangerous. It is better to let authors speak for themselves and call taxonomies that which we consider categorizations, lest we put words in their mouths.

We believe that there is a fundamental difference between the lists of system vulnerabilities or individual incidents that have appeared in the literature and a common language or a typology for describing and classifying or categorizing the fuller range of computer-related incidents. The categorization system we are seeking is one that helps administrators to understand incidents that target individuals, those that target systems (about which much has been written), and also incidents that target data and/or intellectual property. Managers of information systems, and certainly the executive officers of an organization, must be aware of all three categories of incidents and the risks each type brings to the IT group and the college or university. Therefore, we must better understand the different types, and the factors leading to the occurrence of each, to improve the security of our systems and our responses to the incidents once they occur.

As described previously, in practice, colleges and universities have increasingly categorized incidents for efficient response and aggregation of data. Howard (1997) cites Cohen (1995), who describes lists of incidents (e.g.: Trojan horses, time bombs, data diddling, backup theft), adding, “a complete list of the things that can go wrong with information systems is impossible to create…. [T]here are a potentially infinite number of different problems that can be encountered, so any list can only serve a limited purpose.”\(^{41}\)

The CERT Guide to System and Network Security Practices, written by Julia H. Allen, provides a comprehensive coverage of procedures for “hardening and securing the system”, and for providing “intrusion detection and response.”\(^{42}\) Of particular value are the checklists provided by the author for developing policies, putting firewalls into operation, selecting, installing, and understanding tools for response, and others. These

\(^{40}\) For more information on the REN-ISAC, please see <http://ren-isac.net/about.html>.


checklists make this book more than a list of systems or network vulnerabilities. They help administrators begin to see the wider range of dynamic interactions between management practices and computer systems and the ways that those human and organizational processes affect security.

Extending the Aslam et al. (1996) work and also that of the ICAMP I and II projects, Pascal Meunier, a research scientist in the CERIAS laboratory at Purdue University has developed a system for aggregating computer-related incidents and responses thereto.43 The database is one of the first of its kind allowing administrators from different locations to contribute to an aggregated source of anecdotal information regarding computer-related events and the responses that were made to them. Though, due to lack of funding, this effort has not continued with its original intensity, perhaps it has provided a prototype, at least in concept, for continuing efforts by ISACs and other formal and informal information-sharing bodies.

Peter Neumann (1995) created one of the earliest lists of computer-related incidents as the originator of the Internet Risks Forum.44 Neumann’s book, entitled Computer Related Risks,45 is written for a wide audience of people at different levels of computer and network management. In his book, Neumann expands the range of computer-related incidents for the audience by discussing many different categories of incidents. He discusses safety problems due to faulty controllers in transportation systems, threats to privacy such as false arrests due to computer-data name confusions, security and integrity problems with examples of human error, and many others. He helps to define the security-related terms of integrity, confidentiality, and availability, and shows readers how to look at the security aspects of the different incidents that have occurred. Neumann does not set out to create any categorization system, but rather to inculcate in readers a sense of the breadth and depth of potential risks faced in technical and everyday situations. This monograph’s greatest contribution to the literature comes from the conceptual shift the author achieves through raising the consideration of computer-related security issues to a broader focus.

The final version of the NIST Computer Security Incident Handling Guide (Grance et al., 2004) was released in January 2004, having been in the comment stage since September 2003. This is a very valuable document, in that it provides comprehensive coverage of different types of incidents, and for each type provides detection and analysis procedures, as well as containment, eradication, and recovery, and post-incident responses. This document also recognizes different levels of seriousness and helps systems managers know what indications of each level they might see. Unlike many other such documents, this one does not ignore categories of incidents which focus on data, such as unauthorized access and those which focus on people such as email harassments etc. The document provides, for these “inappropriate usage incidents,” definition, examples, and incident handling procedures as well as prevention procedures.

Referring again to the important work of John Howard (1997), this review would not be complete without noting that in this work, Howard writes about attackers and people vis-à-vis their particular objectives. He discusses the motivations of attackers and the objectives of their attacks. He notes that the tools, access privileges, and results fall in between “attackers” and “objectives.” This is a particularly interesting approach and is relevant to the work of the CIFAC project. While we cannot know the motivation and sometimes the objectives of the people who purposefully or accidentally cause incidents on information resources, looking at incidents in this way helps us to focus on target and categorize incidents more broadly. Howard looks at how access for a given attack was achieved, categorizing the vulnerabilities into implementation vulnerability, design vulnerability, and configuration vulnerability. This seems particularly important in that it begins to show how human error can contribute in several ways and perhaps opens the realm of potential responses, beyond what the literature usually addresses, simply systems or network focused responses. Howard also looks at the results of attacks and identifies four main categories: corruption of information, disclosure of information, theft of service, denial of service.

Conclusions Regarding Taxonomies and Categorizations
The need for a clear and robust framework through which to view incidents, their causes, and their management is evinced by the literature and discussions in the CIFAC/EDUCAUSE focus groups. Academics and

44 For more information on the Internet Risks Forum, please see <http://catless.ncl.ac.uk/Risks>.
practitioners have been working on creating such a framework for over a decade, primarily by suggesting taxonomies, lists, and categorizations. Each method has its own strengths and shortcomings.

Taxonomies create clear and logical structures, but they often prove too unwieldy and compartmentalizing for practical application. That no characteristic of an IT incident is inherently a priori any other further mitigates the appropriateness of a taxonomical view of incidents. Lists provide comprehensive coverage of known vulnerabilities, but they do not illustrate any causal, contributory, or prescriptive associations between these vulnerabilities; moreover, they tend to be specific to an operating system, program, hardware configuration, or protocol and therefore do not possess the universality that should be a salient characteristic of any inter-organizational incident discussion framework.

Categorization schemes exist somewhere between taxonomies and lists; they serve to give some order and universality to lists without creating too rigid a system of hierarchies. The beauty of categorization schemes is that they are simultaneously ductile and rigid; they allow institutional modification and adaptation without sacrificing the minimum level of stringency to make them useful across institutions and fields. Categorizations provide guidance for incident handling and management, offer simplicity for easy application, and allow data sharing for analysis purposes without excessively cordoning off incidents based on a particular, and essentially arbitrarily chosen, characteristic. For these reasons, we believe that a categorization system will provide the most value to both technical and non-technical practitioners of incident prevention and management.

Need for Metrics
Our review of the literature shows that the need to recognize and encourage consideration of human motives, objectives, and the impact or results of the incident is increasingly emphasized in current prescriptive literature. It brings the focus of computer-related incidents into more alignment with the work of risk managers and auditors as they seek to protect colleges and universities from risks—from damage and loss. There is an irony in that nearly ten years ago, Neumann was writing about such computer-related incidents and calling his work Computer Related Risks. Now, we are again focusing on the relationship of computer-related incidents and organizational risks. This maturing perspective on incident management is more inclusive, wider, and requires the involvement of others to ensure sufficient organizational perspective and the exercise of best practices.

In 2001, researchers at NIST published the Risk Management Guide for Information Technology Systems. This document provides a foundation for the development of an effective risk management program, containing both definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. Like other documents of NIST it provides clear and helpful recommendations. It encourages organizations to assess the value of their IT assets and proceed with a risk management approach to computer-related incidents.

In 2003, NIST released Special Publication 800-55, entitled Computer Security: Security Metrics Guide for Information Systems. The purpose of this guide was to provide a basis for benefit-cost analysis of various security measures. This work, albeit on a grander scale than the ICAMP I and II studies, is much like those studies – creating metrics that will assist systems administrators and organizational executive officers to understand the economic risks associated with computer incidents. This document illustrates the push within the last few years towards more metrics, more measurement, more codification, more recording, more analysis, and more reporting of data regarding computer-related incidents.

In a 2003 article in the Harvard Business Review, Robert Austin and Christopher Darby emphasize the importance of engaging others, not just technical staff, in handling computer-related incidents. (This work

---

appeared in the *HBR* shortly after Nicholas Carr’s widely-flamed article *Why IT Doesn’t Matter* re-ignited the tendentious debate between technologists and business managers.) Austin and Darby explain:

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.

Like the work at NIST in Special Publication 800-30 (Stoneburner et al., 2001), these authors stress the risk management approach. Significantly, though, this article appears in the nation’s foremost semi-scholarly management journal. This illustrates the movement of IT risk management into mainstream business practice. It also suggests that there could be a benefit obtained by increasing communication between the higher education sector and the business sector regarding the most effective ways to prevent incidents given the specific needs of different organizations’ computers and networks.

Other literature, including that of a technical bent, shows this shift to a more risk management approach and toward the use of metrics in viewing and responding to computer-related incidents. Like Austin and Darby, we realize that companies need to have smart technicians who use lists and taxonomies of vulnerabilities, stay abreast of technical research in their field, and quickly obtain as information, upgrades, and patches from vendors to secure their systems. But the opinion that they should not “be calling the shots” on incident management and response, to quote Austin and Darby, seems to be gaining prominence within colleges and universities and the literature addressing these institutions.

We concur. Systems administrators should not be inappropriately burdened with the role of determining the priority rating that different types of incidents receive on a criticality/seriousness scale, or setting the thresholds for when certain types of incidents get escalated to include others in the incident management and decision-making process. While, in the past the systems and network staff have been alone in understanding how computer-related incidents were happening, we cannot continue to ask them to carry the burden of these decisions, and perform the technical responses that are required as well. Experience and a better understanding of the nature of computer-related incidents has led to a more comprehensive and wider view of incident management, one that does not rely on lists or taxonomies or technicians, but that calls for other tools to assist in this more risk management approach. This new approach involves codification/categorization, defining thresholds for response, and responding through proven best practices.

While they should have a seat at the discussion of incident management, managers must resist the temptation to ascribe more decision making responsibility to their technicians than is appropriate given the mature and mission of the organization. It must never be forgotten that the purpose of the IT group is to support the missions of the college or university: teaching, research, and public service. The mission of the university should guide the needs of faculty and students, which should in turn signal technologists about their role. The mission of the institution should not be determined by technical simplicity, nor should the needs of faculty and students be circumscribed by technical feasibility. Research, teaching, and service should guide technological development and deployment, not vice versa.
Appendix B: CIFAC Instrument

COMPUTER INCIDENT FACTOR ANALYSIS AND CATEGORIZATION
Gerald R. Ford School of Public Policy
The University of Michigan  734-615-9595  o
712 Oakland Street, Room 159  734-998-6688  f
Ann Arbor, MI 48104-3021  cifac.staff@umich.edu

Name _____________________________________________________________
Institution ___________________________________________________________________

Interviewer VR / DR / AK Date _____ / _____ / _____
Setting ___________________________ Day _____________________
Other ___________________________ Time start ___:___ end ___:___

PURPOSE
The purpose of the CIFAC project is to collect information regarding computer-related incidents and to attempt to statistically identify factors that are related to the occurrence of various types of incidents. We hope to be able to recommend best practices for addressing some of these incidents in colleges, universities, and corporations.

DEFINITION
A computer incident is defined as any action or 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 or target individuals, systems, or data resources and result in a policy, education, disciplinary, or technical action.

We need you to name and describe three incidents, from your area of expertise and experience that occurred within the last twelve months.

INCIDENT

Name it:
1
2
3
4

Please briefly DESCRIBE what happened in this incident.
1. How **SERIOUS** would you say this incident was?
   
   (1) not at all
   (2) somewhat
   (3) quite
   (4) extremely

2. In a sentence or two, specifically **WHAT** about this incident made you **SCORE** it this way?

3. Was the primary **FOCUS** of the incident on…?
   
   (1) people
   (2) data
   (3) systems

4. If you could have done one thing to **PREVENT** this incident from having happened, what would it be?

5. To **PREVENT** this incident from happening in the future, how important is increasing the availability of the following **RESOURCES**:
   
   (1) not at all  (2) somewhat  (3) quite  (4) extremely

   - personnel
   - hardware
   - software
   - network
   - physical security
   - access control tools
   - other ______________________________

6. To **PREVENT** this incident from happening in the future, how important is increasing the availability of **TRAINING/EDUCATION** for:

   (1) not at all  (2) somewhat  (3) quite  (4) extremely

   - IT managers
   - faculty
   - students
   - IT staff
   - non-IT staff
   - authorized external users
   - other ______________________________

7. To **PREVENT** this incident from happening in the future, how important is increasing or improving **PROCEDURES** for:

   (1) not at all  (2) somewhat  (3) quite  (4) extremely

   - network management
   - incident response
   - backup/recovery of systems and data
   - documenting systems and networks
   - auditing systems
   - configuring software
   - detecting and patching software bugs
   - other ______________________________
8. To **PREVENT** this incident from happening in the future, how important is the **EXISTENCE** of:

(1) not at all   (2) somewhat   (3) quite   (4) extremely

- backup and recovery
- documentation
- promulgation of documentation and policies
- logging
- analysis of logs
- identification, authentication, and authorization

other ______________________________

9. To **PREVENT** this incident from happening in the future, how important is increasing or improving **REQUIREMENTS** for:

(1) not at all   (2) somewhat   (3) quite   (4) extremely

- IT managers
- IT staff
- use of institutional resources
- use of personal information

other ______________________________

10. To **PREVENT** this incident from happening in the future, how important is the level of **KNOWLEDGE** required, prior to use, for:

(1) not at all   (2) somewhat   (3) quite   (4) extremely

- faculty
- students
- non-IT staff
- authorized external users

other ______________________________

11. To **PREVENT** this incident from happening in the future, how important is increasing or improving **CONFIGURATION** requirements for:

(1) not at all   (2) somewhat   (3) quite   (4) extremely

- networks
- desktop software
- desktop hardware
- server or mainframe hardware
- server or mainframe software

other ______________________________

12. In **CAUSING** this incident to happen, how important was the lack or deficiency of the following **RESOURCES**:

(1) not at all   (2) somewhat   (3) quite   (4) extremely

- personnel
- hardware
- software
- network
- physical security

other ______________________________
13. In **CAUSING** this incident to happen, how important was the lack or deficiency of **TRAINING/EDUCATION** for:

(1) not at all  (2) somewhat  (3) quite  (4) extremely

IT managers
faculty
students
IT staff
non-IT staff
incident investigators
other ______________________________

14. In **CAUSING** this incident to happen, how important was the lack or deficiency of **PROCEDURES** for:

(1) not at all  (2) somewhat  (3) quite  (4) extremely

network management
incident response
backup/recovery of systems and data
documenting systems and networks
auditing systems
other ______________________________

15. In **CAUSING** this incident to happen, how important was the lack or deficiency of **REQUIREMENTS** for:

(1) not at all  (2) somewhat  (3) quite  (4) extremely

IT managers
IT staff
non-IT staff
use of institutional resources
use of personal information
other ______________________________

16. In **CAUSING** this incident to happen, how important was the lack or deficiency in the level of **KNOWLEDGE** required, prior to use, of:

(1) not at all  (2) somewhat  (3) quite  (4) extremely

faculty
students
authorized external users
other ______________________________

17. In **CAUSING** this incident to happen, how important was the lack or deficiency of **CONFIGURATION** requirements for:

(1) not at all  (2) somewhat  (3) quite  (4) extremely

networks
desktop software
desktop hardware
server or mainframe hardware
server or mainframe software
other ______________________________
18. In **CAUSING** this incident to happen, how important was the lack or deficiency of **CONFIGURATION** requirements for:

- networks
- desktop software
- desktop hardware
- server or mainframe hardware
- server or mainframe software
- other ______________________________

19. In **CAUSING** this incident to happen, how important was the **LACK** or deficiency of:

- backup and recovery
- documentation
- promulgation of documentation and policies
- logging
- analysis of logs
- identification, authentication, and authorization
- other ______________________________

20. In **CAUSING** this incident to happen, how important was **ACCIDENTAL** or **CARELESS** behavior of the following:

- IT managers
- faculty
- students
- IT Staff
- non-IT Staff
- authorized or permitted external users
- unauthorized external users
- other ______________________________

21. In **CAUSING** this incident to happen, how important was **MALICIOUS** or **ABUSIVE** behavior of the following:

- IT managers
- faculty
- students
- IT Staff
- non-IT Staff
- authorized or permitted external users
- unauthorized external users
- other ______________________________

22. How **ADEQUATE** were the pre-established **PROCEDURES** for incident response?

- (1) not at all
- (2) somewhat
- (3) quite
- (4) extremely

23. Once the incident was made known, how well **FOLLOWED** were these **PROCEDURES**

- (1) not at all
- (2) somewhat
- (3) quite
- (4) extremely
24. Overall, how **EFFECTIVE** were these **PROCEDURES**? 
   (1) not at all  
   (2) somewhat  
   (3) quite  
   (4) extremely  

25. If you saw this incident starting again, what one thing would you do to **MITIGATE** the incident’s **IMPACT**?

26. In this incident, how important were the following as stimulus to **ACTION**. 
   (1) not at all  
   (2) somewhat  
   (3) quite  
   (4) extremely  
   cost to department, college, or university  
   time involved for resolution  
   number of people affected  
   level, status, or rank of people affected  
   number of machines affected  
   type and sensitivity of data involved  
   types of machine(s) affected  
   probability of further access or damage  
   probability of damage/harm to individuals  
   probability of damage to institutional reputation  
   other  ______________________________

27. Regarding this incident, what **“BEST PRACTICE”** would you share with a colleague…
   … to avoid/prevent the incident  
   … to mitigate the effect of the incident  
   … to manage the incident  

28. Is there anything **ELSE** you would like to **SHARE** with us about this incident or its management

**INSTITUTIONAL DEMOGRAPHICS**

29. Approximately how many **USERS**, including students, faculty, and staff, does your  **IT system support**? (Let them give an estimate – don’t tell the bins.) 
   (1) <= 100  
   (2) > 100 – 500<=  
   (3) > 500 – 1,000<=  
   (4) > 1,000 – 5,000<=  
   (5) > 5,000 – 20,000<=  
   (6) > 20,000 – 50,000<=  
   (7) >50,000

30. How **CENTRALIZED** would you say your systems are? That is, to what extent are they controlled and managed from a central office versus managed locally by schools, colleges, or departments? 
   (1) not at all  
   (2) somewhat  
   (3) quite  
   (4) extremely
31. When an incident is **REPORTED** to an IT staff member, how important is it to… 
(1) not at all  (2) somewhat  (3) quite  (4) extremely
recorded in a database
reported to a departmental office
reported to an institutional office
reported to an external office (e.g., CERT)
discussed with incident management team

32. Are there institutional or organizational **NORMS** that require IT personnel, for certain kinds of incidents, to **INVOLVE** any of the following types of people? 
(0)  no  (1) yes
risk managers
attorneys
auditors
law enforcement
human resources
public relations
student affairs

33. Are there established **POLICIES** that require IT personnel, for certain kinds of incidents, to **INVOLVE** any of the following types of people? 
(0)  no  (1) yes
risk managers
attorneys
auditors
law enforcement
human resources
public relations
student affairs
## Appendix C: Participating Colleges and Universities

<table>
<thead>
<tr>
<th>American University</th>
<th>Santa Clara University</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binghamton University</td>
<td>Southwestern University</td>
</tr>
<tr>
<td>Boston University</td>
<td>Stanford University</td>
</tr>
<tr>
<td>California State University—Monterey Bay</td>
<td>Syracuse University</td>
</tr>
<tr>
<td>Cleary University</td>
<td>The Georgia Institute of Technology</td>
</tr>
<tr>
<td>Concordia University</td>
<td>The Massachusetts Institute of Technology</td>
</tr>
<tr>
<td>Cornell University</td>
<td>The University of California at Berkeley</td>
</tr>
<tr>
<td>Emory University</td>
<td>The University of Chicago</td>
</tr>
<tr>
<td>Georgetown University</td>
<td>The University of Findlay</td>
</tr>
<tr>
<td>Georgia State University</td>
<td>The University of Illinois at Chicago</td>
</tr>
<tr>
<td>Hampshire College</td>
<td>The University of Maryland, Baltimore County</td>
</tr>
<tr>
<td>Lake Forest College</td>
<td>The University of Maryland, College Park</td>
</tr>
<tr>
<td>LeMoyne College</td>
<td>The University of Massachusetts, Amherst</td>
</tr>
<tr>
<td>Loyola University of Chicago</td>
<td>The University of Massachusetts, Boston</td>
</tr>
<tr>
<td>Michigan State University</td>
<td>The University of Michigan, Dearborn</td>
</tr>
<tr>
<td>Northwestern University</td>
<td>The University of Michigan, Flint</td>
</tr>
<tr>
<td>Saginaw Valley State University</td>
<td>The University of Texas at Austin</td>
</tr>
<tr>
<td>San José State University</td>
<td>The University of Texas at San Antonio</td>
</tr>
</tbody>
</table>
Appendix D: Sample of CIFAC Computer-Related Incidents

A brief sample of the incidents collected in the CIFAC study is provided below. It is our intent to publish a more complete sample of incidents following the completion and publication of Volume II.

**GAO Bot Outbreak in Dorms**

We had approximately 1500 virus incidents in the dorm. About 1000 came into play in the dorms during that time. It was very hard to get these cleaned off of the machines. The students didn’t have patches. They shared files more than needed. The GAO bot is a blended virus which infects machines in a variety of ways. It looks for common passwords, looks for common vendor vulnerabilities, spreads itself through open shares on the vendor networking. Once a machine is infected it seeks to infect other machines. The residence hall IT consultants turned off ports by the hundreds. This incident happened during finals at the end of March.

**Ebay Scammer**

The subject received a complaint through the infrastructure techs from someone not affiliated with the university telling that they had bought and paid for computer games on eBay, but had only an empty box sent to them. The fine print on the eBay listing did say that it was boxes only, not games. The buyer contacted eBay and the university about this perceived scam. Upon investigation, the fine print was found and it was also found that the seller had not been a student in over a year and a half—but her account was left open. The account was closed as soon as this was discovered; however, it was discovered that the student was married and it seems that the student’s husband had also been a student. It appears that the husband of the student (a day trader by trade) had used her account without her consent. They have been unable to find information about the husband and have thus not contacted him; He did not use his account for any of these transactions, so they cannot do anything to his account.

**LDAP Mining**

Many students on the campus received email soliciting their participation in a study. It was found that someone had gone through the LDAP server and extracted information on multiple users then sent them specific information. The person was found to have been a faculty member on an affiliated campus of the university. The faculty member wanted to solicit student participants for a research study.

**IDNOs**

Duplicate IDNOs (personal identification master numbers) were found in the registration system. Each individual has a IDNO but it is kept secret. In this incident, a student was found with two sets of records. Usually what happens is that people come back in a separate position; a creation of a duplicate IDNO occurs through miskeying, name change, etc. This was found to be the case in this incident as well.

**Power Problem**

Our data center UPS solution is not connected to a generator. Whenever the campus power grid experiences failure, we only have a limited amount of battery sustainability before the room looses power and crashes. This costs us a fortune. Staff members have to do an orderly shut down of the data center before the system crashes. Shut down is between 10 hours to three days. Whenever they perform maintenance on the power grid, we are totally dependent upon 15 year old UPS technology. It does not have an alert for when there are problems. This technology is very difficult to maintain and service because of difficulty in getting parts. If there were a generator, the stress on the UPS would be lessened.

**Blackboard**

Person went to take their quiz and found that it had already been taken. She approached the teacher and said that she thought she knew who had taken her quiz. The professor contacted the IT department and asked if there was a way to track this action. The staff member looked at the logs and examined the email of the suspected individual to see if there was any evidence. The processor also confronted the suspected individual and the person confessed.
Corruption of data in the warehouse

Data extracts from transaction systems, during an upgrade, were not properly migrated to the data warehouse. This resulted in several months of undetected data missing from the warehouse—over 90 days.

Defacing a Web Site

Over a weekend, a website was defaced and replaced with something embarrassing. This was a website of some service or department run at the university. It was used by students quite actively. The computing center was notified. The website owner was notified first. The investigation showed that the web server was not in the computing center. It was not being managed for security on the system or the network on which it resided. It was not being monitored as well as it should have been. The staff did not find out who did this but restored the website from a backup. The website was moved behind a firewall and put into the computing center where it is currently being managed.

Nasty IRC worm

A nasty IRC worm infected student computers through WiFi network. The WiFi network is pervasive throughout the campus. The subject’s office had to find a way to provide quarantine folders for when infected students connect. When IDS detects attack they are manually sent to a quarantine fold for new DAT files. There are different levels of disabling depending on the possibility of the end users fixing the problem themselves. Last month there were 200 of these infections.

Admissions and Records Error

An employee in the Admissions and Registration department inadvertently posted 3000 names, addresses, and Social Security numbers of current and prospective students to a publicly accessible folder in her directory.

Email Addresses Leaked

Someone go hold of a set of email addresses. They wanted to communicate with a wide population of the university regarding buying back textbooks. The addresses are published in the paper directory. The process is not allowed from electronic resources. It was found that the email addresses were obtained by someone external to the University.

Email Identity Abuse

A staff member at the school received returned email regarding child pornography. She did not send the original email. She was very upset about the message and reported it to the system administrator in her office. The complaint was forwarded on to the Vice President because the woman was so upset. She indicated that she was being spammed again and that the mail, about little boys, was going out in her name. She did not want it associated with her name. She considered the material coming back to her to be spam. The material coming back to her was bounced electronic mail. The content was the most upsetting to her because her name was associated with it. At a certain level, we all get spam of this nature, and tend to disregard it. When it is coming from someone else we put it into out trash. The fact that this was coming from what appeared to be her own name, made this a different response.

Sharing Access

A person gave his credentials to another employee to do a payroll function. A new person came in and was in training. The person who usually did the payroll function was training the new employee. The trainer told her where she could find his secure ID and password.

Spidering

We received an email message from [redacted].COM. What had happened was that from a particular IP address located on university property, 23,000 requests were processed in eight minutes. Requests were for pages from another source. It turned out that in the library there were a couple of thousand ports where anyone can come in and get on to the Internet. We did not find the culprit but we did find the location. It was stopped.
Appendix E: Statistical Analysis

Documentation of results from data reduction procedure: Factor Analysis, Non Parametric Correlations: Relationships among factors, Scales from FA Internal Consistency: Reliability Analysis.

**Factor Analysis** setting the loading coefficients at greater than or equal to 0.57, as a mean of reducing the 87 prevention and cause variables into factors with a total of less than 31 variables, to increase inferential power for results of statistical analyses.
<table>
<thead>
<tr>
<th>Component</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITstaffcsedu</td>
<td>.804</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITmanagercsedu</td>
<td>.759</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>itstaffsaccdt</td>
<td>.755</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITstaffcsreq</td>
<td>.746</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITstaffpvreq</td>
<td>.745</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>itmanagersaccdt</td>
<td>.734</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITstaffpvedu</td>
<td>.726</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITmanagerpvreq</td>
<td>.723</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITmanagercsreq</td>
<td>.682</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITmanagerspvedu</td>
<td>.660</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>studentcltnpvkw</td>
<td>.820</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>studentcltncsvk</td>
<td>.812</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>studentcltncsedu</td>
<td>.788</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>studentcltnpvedu</td>
<td>.770</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>facultycsedu</td>
<td>.749</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>facultypvkw</td>
<td>.719</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>facultycskw</td>
<td>.712</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>facultypvedu</td>
<td>.697</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>studentcltnscaccdt</td>
<td>.662</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>networkpvconfig</td>
<td>.736</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>networkcsrs</td>
<td>.723</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>networkpvrs</td>
<td>.704</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>networkmgcsproc</td>
<td>.636</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ntwkmgpvproc</td>
<td>.630</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noITstaffcsedu</td>
<td>.732</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noITstaffcsreq</td>
<td>.720</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noitstaffsaccdt</td>
<td>.681</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noITstaffpvkw</td>
<td>.621</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a- Rotation converged in 10 iterations.
Non Parametric Spearman Rho relationships analyses, between the variables with loading coefficients of 0.57 or above in FA.

**Factor 1 - IT Personnel Factor: Education, Requirements, Accidental Behavior**

<table>
<thead>
<tr>
<th>IT Personnel**</th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
<th>4.</th>
<th>5.</th>
<th>6.</th>
<th>7.</th>
<th>8.</th>
<th>9.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Prevention Education for IT Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Prevention Education for IT Staff</td>
<td>.790</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Cause Education for IT Manager</td>
<td>.662</td>
<td>.619</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Cause Education for IT Staff</td>
<td>.568</td>
<td>.722</td>
<td>.800</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Prevention Requirement IT Manager</td>
<td>.609</td>
<td>.576</td>
<td>.669</td>
<td>.539</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Prevention Requirement IT Staff</td>
<td>.535</td>
<td>.655</td>
<td>.584</td>
<td>.622</td>
<td>.857</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Cause Requirement IT Manager</td>
<td>.528</td>
<td>.487</td>
<td>.707</td>
<td>.613</td>
<td>.714</td>
<td>.622</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Cause Requirement IT Staff</td>
<td>.452</td>
<td>.546</td>
<td>.616</td>
<td>.724</td>
<td>.603</td>
<td>.670</td>
<td>.778</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Cause Accidental Behavior IT Manager</td>
<td>.455</td>
<td>.416</td>
<td>.610</td>
<td>.536</td>
<td>.544</td>
<td>.493</td>
<td>.647</td>
<td>.555</td>
</tr>
<tr>
<td>10.</td>
<td>Cause Accidental Behavior IT Staff</td>
<td>.357</td>
<td>.482</td>
<td>.531</td>
<td>.625</td>
<td>.421</td>
<td>.466</td>
<td>.498</td>
<td>.548</td>
</tr>
</tbody>
</table>

**Correlation is significant at the 0.01 level (2-tailed).**

**Factor 2 - Academic Users Factor: Education, Knowledge, Accidental Behavior.**

<table>
<thead>
<tr>
<th>Academic Users**</th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
<th>4.</th>
<th>5.</th>
<th>6.</th>
<th>7.</th>
<th>8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Prevention Education for Faculty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Prevention Education for Students</td>
<td>.556</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Cause Education for Faculty</td>
<td>.665</td>
<td>.427</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Cause Education for Students</td>
<td>.388</td>
<td>.787</td>
<td>.505</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Prevention Knowledge Faculty</td>
<td>.708</td>
<td>.439</td>
<td>.745</td>
<td>.399</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Prevention Knowledge Students</td>
<td>.486</td>
<td>.771</td>
<td>.494</td>
<td>.779</td>
<td>.578</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Cause Knowledge Faculty</td>
<td>.580</td>
<td>.363</td>
<td>.792</td>
<td>.418</td>
<td>.707</td>
<td>.438</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Cause Knowledge Students</td>
<td>.392</td>
<td>.742</td>
<td>.497</td>
<td>.863</td>
<td>.411</td>
<td>.788</td>
<td>.508</td>
</tr>
</tbody>
</table>

**Correlation is significant at the 0.01 level (2-tailed).**

**Factor 3 - Network Factor: Resources, Procedures, Configuration.**
<table>
<thead>
<tr>
<th>Network**</th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
<th>4.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Prevention Availability of Network Resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Cause Availability of Network Resources</td>
<td>.589</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Prevention Procedures for Network Management</td>
<td>.448</td>
<td>.452</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Prevention Configuration Requirements for Networks</td>
<td>.505</td>
<td>.585</td>
<td>.701</td>
<td>.592</td>
</tr>
</tbody>
</table>

** Correlation is significant at the 0.01 level (2-tailed).

Factor 4 - Non IT Staff Factor: Education, Requirements, Awareness/Knowledge, Accidental Behavior.

<table>
<thead>
<tr>
<th>Non IT Staff**</th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Prevention Awareness of Requirements for Non IT Staff</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Cause Education for Non IT Staff</td>
<td>.668</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Cause Requirement Non IT Staff</td>
<td>.447</td>
<td>.605</td>
<td></td>
</tr>
<tr>
<td>4. Cause Accidental Behavior Non IT Staff</td>
<td>.471</td>
<td>.609</td>
<td>.611</td>
</tr>
</tbody>
</table>

** Correlation is significant at the 0.01 level (2-tailed).

Reliability Analysis to verify internal consistency of scales created with items from FA.

Scale 1 - IT Personnel Scale: Education, Requirements, Accidental Behavior.

| Item Statistics |
|---|---|---|
| Mean | Std. Deviation | N |
| ITmanagerspv edu | 2.28 | 1.065 | 304 |
| ITstaffpv edu | 2.45 | 1.064 | 304 |
| ITmanagerpv req | 1.82 | .949 | 304 |
| ITstaffpv req | 1.97 | 1.008 | 304 |
| ITmanagercsc edu | 1.82 | .973 | 304 |
| ITstaffcsc edu | 1.96 | 1.057 | 304 |
| ITmanagerscsreq | 1.59 | .889 | 304 |
| ITstaffcsreq | 1.71 | .965 | 304 |

| Reliability Statistics |
|---|---|
| Cronbach's Alpha | N of Items |
| .936 | 10 |
### Item-Total Statistics

<table>
<thead>
<tr>
<th></th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITmanagerspvedu</td>
<td>16.37</td>
<td>49.620</td>
<td>.690</td>
<td>.932</td>
</tr>
<tr>
<td>ITstaffpvedu</td>
<td>16.20</td>
<td>48.993</td>
<td>.737</td>
<td>.930</td>
</tr>
<tr>
<td>ITmanagerpvreq</td>
<td>16.83</td>
<td>49.916</td>
<td>.768</td>
<td>.928</td>
</tr>
<tr>
<td>ITstaffpreq</td>
<td>16.68</td>
<td>49.411</td>
<td>.754</td>
<td>.929</td>
</tr>
<tr>
<td>ITmanagersedu</td>
<td>16.83</td>
<td>49.011</td>
<td>.818</td>
<td>.926</td>
</tr>
<tr>
<td>ITstaffcsedu</td>
<td>16.69</td>
<td>48.037</td>
<td>.816</td>
<td>.926</td>
</tr>
<tr>
<td>ITmanagercsreq</td>
<td>17.06</td>
<td>50.514</td>
<td>.776</td>
<td>.928</td>
</tr>
<tr>
<td>ITstaffcsreq</td>
<td>16.94</td>
<td>49.716</td>
<td>.769</td>
<td>.928</td>
</tr>
<tr>
<td>itmanagerscsaccdt</td>
<td>17.18</td>
<td>51.761</td>
<td>.682</td>
<td>.932</td>
</tr>
<tr>
<td>itstaffcsaccdt</td>
<td>17.07</td>
<td>51.546</td>
<td>.640</td>
<td>.934</td>
</tr>
</tbody>
</table>

* Since the scale statistic is above 0.90 we tested alternative subscales as means of increasing reliability.

* Scale 1a - IT Personnel Scale: Education.

### Item Statistics

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITmanagerspvedu</td>
<td>2.27</td>
<td>1.065</td>
<td>311</td>
</tr>
<tr>
<td>ITstaffpvedu</td>
<td>2.44</td>
<td>1.064</td>
<td>311</td>
</tr>
<tr>
<td>ITmanagercsedu</td>
<td>1.81</td>
<td>.968</td>
<td>311</td>
</tr>
<tr>
<td>ITstaffcsedu</td>
<td>1.95</td>
<td>1.054</td>
<td>311</td>
</tr>
</tbody>
</table>

### Item-Total Statistics

<table>
<thead>
<tr>
<th></th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITmanagerspvedu</td>
<td>6.20</td>
<td>7.715</td>
<td>.752</td>
<td>.882</td>
</tr>
<tr>
<td>ITstaffpvedu</td>
<td>6.03</td>
<td>7.473</td>
<td>.807</td>
<td>.862</td>
</tr>
<tr>
<td>ITmanagercsedu</td>
<td>6.66</td>
<td>8.063</td>
<td>.781</td>
<td>.872</td>
</tr>
<tr>
<td>ITstaffcsedu</td>
<td>6.52</td>
<td>7.650</td>
<td>.778</td>
<td>.872</td>
</tr>
</tbody>
</table>

* Scale 1b - IT Personnel Scale: Requirements.
### Reliability Statistics

<table>
<thead>
<tr>
<th>Cronbach's Alpha</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>.900</td>
<td>4</td>
</tr>
</tbody>
</table>

### Item Statistics

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITmanagerpvreq</td>
<td>1.82</td>
<td>.948</td>
<td>305</td>
</tr>
<tr>
<td>ITstaffpvreq</td>
<td>1.97</td>
<td>1.006</td>
<td>305</td>
</tr>
<tr>
<td>ITmanagerscsreq</td>
<td>1.59</td>
<td>.888</td>
<td>305</td>
</tr>
<tr>
<td>ITstaffcsreq</td>
<td>1.71</td>
<td>.964</td>
<td>305</td>
</tr>
</tbody>
</table>

### Item-Total Statistics

<table>
<thead>
<tr>
<th></th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITmanagerpvreq</td>
<td>5.27</td>
<td>6.386</td>
<td>.808</td>
<td>.859</td>
</tr>
<tr>
<td>ITstaffpvreq</td>
<td>5.12</td>
<td>6.216</td>
<td>.783</td>
<td>.868</td>
</tr>
<tr>
<td>ITmanagerscsreq</td>
<td>5.50</td>
<td>6.797</td>
<td>.771</td>
<td>.873</td>
</tr>
<tr>
<td>ITstaffcsreq</td>
<td>5.37</td>
<td>6.544</td>
<td>.747</td>
<td>.881</td>
</tr>
</tbody>
</table>

* Scale 1c - IT Personnel Scale: Accidental Behavior.

### Reliability Statistics

<table>
<thead>
<tr>
<th>Cronbach's Alpha</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>.842</td>
<td>2</td>
</tr>
</tbody>
</table>

### Item Statistics

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>itmanagerscsaccdt</td>
<td>1.45</td>
<td>.865</td>
<td>313</td>
</tr>
<tr>
<td>itstaffcsaccdt</td>
<td>1.56</td>
<td>.935</td>
<td>313</td>
</tr>
</tbody>
</table>

### Item-Total Statistics

<table>
<thead>
<tr>
<th></th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>itmanagerscsaccdt</td>
<td>1.56</td>
<td>.875</td>
<td>.729</td>
<td>.879</td>
</tr>
<tr>
<td>itstaffcsaccdt</td>
<td>1.45</td>
<td>.749</td>
<td>.729</td>
<td>.879</td>
</tr>
</tbody>
</table>

* The value is negative due to a negative average covariance among items. This violates reliability model assumptions. You may want to check item codings.

Scale 2 - Academic Users Scale: Education, Knowledge, Accidental Behavior.
## Reliability Statistics

<table>
<thead>
<tr>
<th>Cronbach's Alpha</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>.921</td>
<td>9</td>
</tr>
</tbody>
</table>

### Item Statistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>facultypvedu</td>
<td>2.12</td>
<td>1.172</td>
<td>306</td>
</tr>
<tr>
<td>studentcltnpvedu</td>
<td>2.33</td>
<td>1.233</td>
<td>306</td>
</tr>
<tr>
<td>facultypvkw</td>
<td>1.82</td>
<td>1.077</td>
<td>306</td>
</tr>
<tr>
<td>studentcltnpvkw</td>
<td>2.10</td>
<td>1.156</td>
<td>306</td>
</tr>
<tr>
<td>studentcltncesedu</td>
<td>2.02</td>
<td>1.229</td>
<td>306</td>
</tr>
<tr>
<td>facultycSEDu</td>
<td>1.66</td>
<td>1.048</td>
<td>306</td>
</tr>
<tr>
<td>facultYeskW</td>
<td>1.54</td>
<td>.979</td>
<td>306</td>
</tr>
<tr>
<td>studentcltnceskw</td>
<td>1.91</td>
<td>1.191</td>
<td>306</td>
</tr>
<tr>
<td>studentcltncesacd</td>
<td>1.82</td>
<td>1.167</td>
<td>306</td>
</tr>
</tbody>
</table>

* Since the scale statistic is above .90 we tested alternative subscales as means of increasing reliability.

* Scale 2 - Academic Users Scale: Education.

### Item-Total Statistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>facultypvedu</td>
<td>15.20</td>
<td>52.611</td>
<td>.636</td>
<td>.918</td>
</tr>
<tr>
<td>studentcltnpvedu</td>
<td>14.99</td>
<td>50.102</td>
<td>.755</td>
<td>.910</td>
</tr>
<tr>
<td>facultypvkw</td>
<td>15.50</td>
<td>53.123</td>
<td>.670</td>
<td>.915</td>
</tr>
<tr>
<td>studentcltnpvkw</td>
<td>15.22</td>
<td>50.237</td>
<td>.807</td>
<td>.906</td>
</tr>
<tr>
<td>studentcltncesedu</td>
<td>15.30</td>
<td>49.541</td>
<td>.795</td>
<td>.907</td>
</tr>
<tr>
<td>facultycSEDu</td>
<td>15.66</td>
<td>52.827</td>
<td>.714</td>
<td>.913</td>
</tr>
<tr>
<td>facultYeskW</td>
<td>15.78</td>
<td>54.275</td>
<td>.664</td>
<td>.916</td>
</tr>
<tr>
<td>studentcltnceskw</td>
<td>15.41</td>
<td>49.738</td>
<td>.812</td>
<td>.906</td>
</tr>
<tr>
<td>studentcltncesacd</td>
<td>15.50</td>
<td>52.900</td>
<td>.621</td>
<td>.919</td>
</tr>
</tbody>
</table>

### Item Statistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>facultypvedu</td>
<td>2.13</td>
<td>1.174</td>
<td>310</td>
</tr>
<tr>
<td>studentcltnpvedu</td>
<td>2.33</td>
<td>1.233</td>
<td>310</td>
</tr>
<tr>
<td>studentcltncesedu</td>
<td>2.03</td>
<td>1.230</td>
<td>310</td>
</tr>
<tr>
<td>facultycSEDu</td>
<td>1.66</td>
<td>1.051</td>
<td>310</td>
</tr>
<tr>
<td>studentcltncesacd</td>
<td>1.82</td>
<td>1.168</td>
<td>310</td>
</tr>
</tbody>
</table>

80
### Scale 2 - Academic Users Scale: Knowledge

<table>
<thead>
<tr>
<th>Item-Total Statistics</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>facultypvedu</td>
<td>7.83</td>
<td>14.826</td>
<td>.571</td>
<td>.838</td>
</tr>
<tr>
<td>studentcltnpvedu</td>
<td>7.63</td>
<td>13.101</td>
<td>.755</td>
<td>.787</td>
</tr>
<tr>
<td>studentcltncsedu</td>
<td>7.93</td>
<td>13.028</td>
<td>.768</td>
<td>.784</td>
</tr>
<tr>
<td>facultycsedu</td>
<td>8.30</td>
<td>15.374</td>
<td>.593</td>
<td>.832</td>
</tr>
<tr>
<td>studentcltncsedt</td>
<td>8.14</td>
<td>14.657</td>
<td>.597</td>
<td>.831</td>
</tr>
</tbody>
</table>

### Reliability Statistics

<table>
<thead>
<tr>
<th>Cronbach's Alpha</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>.859</td>
<td>5</td>
</tr>
</tbody>
</table>

### Item Statistics

<table>
<thead>
<tr>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>facultypvkw</td>
<td>1.81</td>
<td>1.075</td>
</tr>
<tr>
<td>studentcltnpvkw</td>
<td>2.09</td>
<td>1.156</td>
</tr>
<tr>
<td>facultycskw</td>
<td>1.53</td>
<td>.976</td>
</tr>
<tr>
<td>studentcltncskw</td>
<td>1.91</td>
<td>1.189</td>
</tr>
<tr>
<td>studentcltncsedt</td>
<td>1.81</td>
<td>1.165</td>
</tr>
</tbody>
</table>

### Scale 3 - Network Scale: Resources, Procedures, Configuration

<table>
<thead>
<tr>
<th>Item-Total Statistics</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>facultypvkw</td>
<td>7.35</td>
<td>13.934</td>
<td>.593</td>
<td>.849</td>
</tr>
<tr>
<td>studentcltnpvkw</td>
<td>7.06</td>
<td>12.230</td>
<td>.778</td>
<td>.801</td>
</tr>
<tr>
<td>facultycskw</td>
<td>7.63</td>
<td>14.404</td>
<td>.607</td>
<td>.846</td>
</tr>
<tr>
<td>studentcltncskw</td>
<td>7.25</td>
<td>11.929</td>
<td>.792</td>
<td>.797</td>
</tr>
<tr>
<td>studentcltncsedt</td>
<td>7.34</td>
<td>13.282</td>
<td>.614</td>
<td>.845</td>
</tr>
</tbody>
</table>

### Reliability Statistics

<table>
<thead>
<tr>
<th>Cronbach's Alpha</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>.853</td>
<td>5</td>
</tr>
</tbody>
</table>

### Item Statistics

<table>
<thead>
<tr>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>networkpvrs</td>
<td>1.47</td>
<td>.862</td>
</tr>
<tr>
<td>ntwkmgpvprom</td>
<td>1.91</td>
<td>1.073</td>
</tr>
<tr>
<td>networkpvconfig</td>
<td>1.87</td>
<td>1.063</td>
</tr>
<tr>
<td>networkcsrs</td>
<td>1.39</td>
<td>.811</td>
</tr>
<tr>
<td>networkmngcsproc</td>
<td>1.53</td>
<td>.911</td>
</tr>
</tbody>
</table>
## Item-Total Statistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>networkpvrs</td>
<td>6.70</td>
<td>10.230</td>
<td>.589</td>
<td>.842</td>
</tr>
<tr>
<td>ntwkmgpvpvproc</td>
<td>6.27</td>
<td>8.682</td>
<td>.694</td>
<td>.817</td>
</tr>
<tr>
<td>networkpvconfig</td>
<td>6.30</td>
<td>8.397</td>
<td>.762</td>
<td>.796</td>
</tr>
<tr>
<td>networkcsrs</td>
<td>6.78</td>
<td>10.117</td>
<td>.682</td>
<td>.825</td>
</tr>
<tr>
<td>networkmgesproc</td>
<td>6.64</td>
<td>9.757</td>
<td>.639</td>
<td>.830</td>
</tr>
</tbody>
</table>

Scale 4 – Non-IT Staff Scale: Education, Requirements, Knowledge, Accidental Behavior.

## Reliability Statistics

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cronbach's Alpha</td>
<td>.850</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

## Item Statistics

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>noITstaffpvkw</td>
<td>2.10</td>
<td>1.144</td>
<td>305</td>
</tr>
<tr>
<td>noITstaffcsedu</td>
<td>2.07</td>
<td>1.173</td>
<td>305</td>
</tr>
<tr>
<td>noITstaffcsreq</td>
<td>1.61</td>
<td>.988</td>
<td>305</td>
</tr>
<tr>
<td>noiTstaffcsaccdt</td>
<td>1.70</td>
<td>1.055</td>
<td>305</td>
</tr>
</tbody>
</table>

## Item-Total Statistics

<table>
<thead>
<tr>
<th></th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>noITstaffpvkw</td>
<td>5.38</td>
<td>7.834</td>
<td>.630</td>
<td>.836</td>
</tr>
<tr>
<td>noITstaffcsedu</td>
<td>5.41</td>
<td>6.946</td>
<td>.785</td>
<td>.766</td>
</tr>
<tr>
<td>noITstaffcsreq</td>
<td>5.87</td>
<td>8.345</td>
<td>.676</td>
<td>.817</td>
</tr>
<tr>
<td>noiTstaffcsaccdt</td>
<td>5.78</td>
<td>8.006</td>
<td>.680</td>
<td>.814</td>
</tr>
</tbody>
</table>
Appendix F: Best Practice Scoring Scales

• Scale for Scoring PREVENTION Best Practices

The scale that was used to score the suggested PREVENTION BEST PRACTICES included the following categories:

1. **Nothing** – Response indicates that there was no preventative measure that would have had a substantial likelihood of preventing or materially reducing the effect of the incident occurring. Key words include “nothing”, “no way,” or “unavoidable.”

2. **Education, training, awareness, and straightforwardness** – Response indicates that educating users, incident handlers, or another relevant body that the institution can reasonably expect to reach would have had a substantial likelihood of preventing or materially reducing the effect of the incident occurring. Keywords include: “education,” “training,” “awareness,” “straightforwardness,” “communication with user community,” “discussion,” “remind,” or “campaign.”

3. **Test, patch, debug, and procedures therefore** – Response indicates that maintaining current software that has been tested and thoroughly debugged would have had a substantial likelihood of preventing or materially reducing the effect of the incident occurring. Also included are standards and policies to regularly or systematically undertake these functions. Keywords included: “test,” “patch,” “debug,” “change management,” “pre-production,” “auditing,” “checks and balances,” “configuration,” “check,” “up-to-date,” and “checklist.”

4. **Have and follow procedures, policies, and standards** – Responses indicated that having and following procedures, policies, and standards would have had a substantial likelihood of preventing or materially reducing the effect of the incident occurring. Also included are the enforcement of policies, including a mechanism for sanctioning violaters. Improving or revising procedures and policies is also included in this section. Keywords include “procedure,” “policy,” “standard,” “AP,” “password (strong or changing),” “antivirus (policy for use),” “requirements,” “data management,” “process map,” “appropriate access level.”

5. **Technical preventative controls** – Responses indicate that technical measures instituted by a local or central IT service would have had a substantial likelihood of preventing or materially reducing the effect of the incident occurring. Key words include: “firewall,” “IDS,” “IPS,” “quarantine,” “ACL,” “automated enforcement,” “antivirus (at the server or router level),” “bandwidth control,” “packet shaping,” “authentication (stronger or two-form),” “encryption,” “identity confirmation,” and “access control.”

9. **Missing or Don’t Know** – Either there were no best practices given or the response indicated that the respondent did not know of a best practices for preventing this incident.

• Scale for Scoring MITIGATION Best Practices

The scale that was used to score the suggested MITIGATION BEST PRACTICES included the following categories:

1. **Administrative collaboration and communication** – Response indicates that cooperation and a collaborative environment between relevant administrative departments at the institution would have likely significantly reduced the impact of an incident on users and/or on the institution. Having open lines of communication between relevant departments and having pre-existing interdepartmental incident response procedures and teams in place are examples of this. Departments frequently cited include IT, student affairs, residential life, legal affairs, risk managers, auditors, campus safety, police, and public relations. May be related only to communication within IT department. Keywords include “interdepartmental,” “appropriate persons,” “the right people,” “interdepartmental IRT,” “working relationships,” “proper relationships,” “efficient communication,” and “clear lines of communication/command.”
2. **Education, training, awareness, and straightforwardness** – Response indicates that educating users, incident handlers, or another relevant body that the institution can reasonably expect to reach would have had a substantial likelihood of preventing or materially reducing the effect of the incident occurring. Keywords include “education,” “training,” “awareness,” “straightforwardness,” “communication (with user community),” “discussion,” “openness,” “straightforward communication,” “talk with victim,” “close contact,” and “regular updates.”

3. **Take decisive and timely action** – Response indicates that speed is paramount in response in order to likely significantly reduce the impact of an incident on users and/or on the institution. Frequently cited in conjunction with other practices especially removal and quarantine. Keywords include “fast,” “quick,” “immediate,” “timely,” “as soon as possible,” and “aggressive.”

4. **Have and follow procedures, policies, and standards** – Response indicates that having and following procedures, policies, and standards would have had a substantial likelihood of preventing or materially reducing the effect of the incident occurring. Also included are the enforcement of policies, including a mechanism for sanctioning violators. Improving or revising procedures and policies is also included in this section. Keywords include “procedure,” “policy,” “standard,” “requirements,” “data management,” “process map,” and “appropriate access level.”

5. **Remove or quarantine cause of problem** – Response indicates that the removal of a problem person or machine would have likely significantly reduced the impact of an incident on users and/or the institution. Keywords include “remove from the network,” “quarantine,” “isolate,” “block access,” “block port,” “null route,” “cut off access,” “divert traffic,” “(v)ACL,” “pull the plug,” and “disable.”

9. **Missing or Don’t Know** – Either there were no best practices given or the response indicated that the respondent did not know of a best practices for mitigating this incident

**Scale for Scoring MANAGEMENT Best Practices**

The scale that was used to score the suggested MANAGEMENT BEST PRACTICES included the following categories:

1. **Administrative collaboration and communication** – Response indicates that cooperation and a collaborative environment between relevant administrative departments at the institution would have likely significantly reduced the impact of an incident on users and/or on the institution. Having open lines of communication between relevant departments and having pre-existing interdepartmental incident response procedures and teams in place are examples of this. Departments frequently cited include IT, student affairs, residential life, legal affairs, risk managers, auditors, campus safety, police, and public relations. May be related only to communication within the IT department. Key words include “interdepartmental,” “appropriate persons,” “the right people,” “interdepartmental IRT,” “working relationships,” “proper relationships,” “efficient communication,” and “clear line of communication/command.” (The orientation in number 1 is unit and department focused.)

2. **Education, training, awareness, and straightforwardness** – Response indicates that cooperation and a collaborative environment between relevant administrative departments at the institution would have likely significantly reduced the impact of an incident on users and/or on the institution. Having open lines of communication between relevant departments and having pre-existing interdepartmental incident response procedures and teams in place are examples of this. Departments frequently cited include IT, student affairs, residential life, legal affairs, risk managers, auditors, campus safety, police, and public relations. May be related only to communication within the IT department. Key words include “interdepartmental,” “appropriate persons,” “the right people,” “interdepartmental IRT,” “working relationships,” “proper relationships,” “efficient communication,” and “clear line of communication/command.” Additional key words include: “openness,” “straightforward communication,” “close contact,” and “regular updates.” (The orientation in number 2 is individual and user focused.)
3. **Take decisive and timely action** – Response indicates that speed is paramount in response in order to likely significantly reduce the impact of an incident on users and/or on the institution. Frequently cited in conjunction with other practices, especially removal and quarantine. Keywords include “fast,” “quick,” “immediate,” “timely,” “as soon as possible,” and “aggressive.”

4. **Have and follow procedures, policies, and standards** – Response indicates that having and following procedures, policies, and standards would have had a substantial likelihood of preventing or materially reducing the effect of the incident occurring. Also included is the enforcement of policies, including a mechanism for sanctioning violators. Improving or revising procedures and policies is also included in this section. Keywords include “procedure,” “policy,” “standard,” “requirements,” “data management,” “process map,” and “appropriate access level.”

5. **Log and document incident** – Response indicates that logging and documenting, either through technical or manual means, the steps leading up to an incident and the procedures taken in its amelioration are an important part of properly managing an incident. Keywords include “documentation,” “logging,” “forensic management,” “write down,” “time stamp,” “accurate records,” and “take notes.”

9. **Missing or Don’t Know** – Either there were no best practices given or the response indicated that the respondent did not know of a best practices for managing this incident
Appendix G: Rationales For Ratings by CIOs

Following are a complete list of the incidents that CIOs from participating schools were asked to rate in terms of seriousness and the rationales that they gave when asked to explain their answers.

**Incident 1: US SECRET SERVICE**

Michael Bush is a second year philosophy and chemistry double major at a small college in Iowa. He has been active on campus and in the community gathering signatures on anti-war petitions, staging rallies, engaging in peaceful civil disobedience. He loves computer games, but doesn't know much about the workings of computers. One day he gets an email from frank.palmer@secretservice.gov informing him that his subversive, anti-American activities have been noted and that he is being monitored very closely.

Michael panics and prints the email, taking it with him to visit an attorney in town who he knows to be sympathetic to his views. The tech-savvy attorney takes one look at the headers and notices that the IP addresses clearly show that the email was sent from a machine on campus. Knowing it is probably a hoax, he phones the college’s IT department to tell them.

Rating: 1
Rationales:
- no immediate danger to people, property, or systems
- since the incident is purely internal and most likely a student prank, it is not a serious threat to the victim or to the campus information resources. The only aspect worth rating attention is the forgery which is an intentional misuse of computing/networking resources

Rating: 2
Rationales:
- there was no system or life threatening incident
- Email spoofing is a known problem
- Spoofing of the email address is, by itself, a slightly serious problem. The fact that the email address is supposed to come from the Secret service makes the consequences more serious for individual and institution.
- not serious except it indicates a lack of possible training for the users.
- that although this is very likely a hoax, certainty has not been determined.
- no direct threat; clearly fraudulent
- events could constitute harassment, Michael probably has irritated more than a few students -a good prank.
- statement of passive action; source IP of email—are we certain campus IP not being used as spoofed email
- forging email is a punishable offense, but beyond that this is really a practical joke
- No apparent immediate danger to anyone or anything; sender violated university policy
- probably a hoax-agreed; student prank and should be responded to but not a serious threat to the individual.
- hoax email; could be spam; No apparent damage to University data or networks.
- misuse of email—violates our acceptable use policy and would get sender to student judicial process
- it came from the campus; it misrepresents a government agency; it singles out a specific person for harassment
- the impersonation of a federal agent and consequences
- no criminal activity or academic misconduct was done; forging email a violation of AUP

Rating: 3
Rationales:
- sending e-mail whose intent to harass an individual- violations of AUP, spoofing return address-using the campus network for fraudulent activities; security threat
- spoofing an apparently off site government address; somewhat threatening nature of the message.
- spoofing US federal agency with intent to intimidate

Rating: 4  N/A
Incident 2: FIRE IN DATA CENTER

Abbey is a third-year Spanish major at a college in North Carolina. Upon returning to campus from winter break she learns that her academic probation has become indefinite academic suspension—probably because of that computer science introductory course that she failed. After expressing her anger, she goes to the nearest cornerstore, and with the help of her mail-order fake ID, buys a pack of beer which she consumes in about three hours. She becomes very drunk. She decides to take a walk on campus and comes near the computer science building. Her proximity card gets her inside and she wanders down to the data center. She lights up a cigarette even though smoking is expressly prohibited in the building. Seconds later, the smoke detector goes off, and water fills the hallway—as well as the data center. Sparks fly and so does Abbey.

Rating: 1 N/A

Rationales:
- accident caused by violating the smoking rules.

Rating: 2

Rationales:
- The urgency is to help the student who appears to need help.
- absolutely drunk; threat to individual; water filled hallway-water may hamper exit by those in building;
- water filled data center-loss of critical infrastructure, data, and university functions; no actual fire which might lead to widespread death and destruction.
- extent of equipment damage; security issue —why does her ID card get her that close to the data center
- not abiding by rules- university property in jeopardy; not reporting the problem -probable loss of property
- privileges card not revoked; administrative systems potential abuse of privileges
- damage to university property
- computers should have been powered out
- very serious because a central resource was compromised by bad design;

Rating: 3

Rationales:
- self-destructive behavior and serious lapse in security. wizards who decided to sprinkler the data center, not a good choice, but Abbeys behavior including smoking is the real issue.
- the college’s network and servers are out of service—extremely serious
- extensive monetary damage
- incredibly serious due to the consequences to the server room
- water in data center-mission critical services in peril,-possibly threatens the operations of the college.
- very serious indicating poor management of the Data Center.
- possible bodily harm;
- impact on data center-what mission critical sources have been affected
- water filling the data center makes this one of the highest priorities; everything in the data center in jeopardy.
- obviously a serious incident with the potential for damage to people and equipment
- apparent loss of entire data center; disruption of information services; apparent serious injury to a person
- water fills the data center —potential damage to critical campus electronics and IT infrastructure
- data center implies that a lot of expensive data is damaged; easy access to important building is of concern;
- computers should have been powered out-not sprinkled
- major system outage
- system described is unrealistic or incorrectly designed
- datacenter probably contains enterprise data; security procedures need serious examination
- Data center is central to all IT services; necessitates immediate response under disaster recovery procedures
Incident 3: DEATH THREAT

Laura Harris and her boyfriend Matt break up after a long relationship. Laura could not believe that Matt would end the relationship. Broken hearted, she begins to think of revenge. She knew Matt’s email password—he had it on a sticky note on his monitor—and so she logged into his email account. She notices a string of correspondence between Matt and her friend, Cat. After reading three of the emails, it becomes painfully clear that Matt has been having an affair for at least three months—with one of her best friends. Laura sends the president of the university an email from Matt’s university account containing a death threat. It is a particularly gory email, omitting no detail of the proposed murder. She cc’s it to a faculty-wide mailing list that was foolishly left un-moderated. Within minutes, the president is on the phone with the police, the FBI, and the IT department. Laura is laughing and standing in the back of the gathered crowd, as she watches a police officer push a handcuffed Matt into the back of a patrol car.

Rating: 1
Rationales:
- This is a human problem and not a security problem. No system issue here.

Rating: 2 N/A

Rating: 3
Rationales:
- very serious due to the people involved; human resources consumed are significant; student email to a faculty-wide un-moderated list is very serious
- no bodily harm imminent; just seriously disruptive threat
- although this case involves seriously inappropriate behavior, it does not rise to the same level of concern as (Fire in the Data Center) -there is neither property damage nor overtly self-destructive behavior involved.
- wrongful accusations-damage to reputation, career, and academic standing; not a bonafide death threat
- death threat; faculty-wide mailing list unmoderated; involvement of the president
- president threatened; threat must be treated as real
- most immediate response has already been provided by law enforcement
- stolen identity and password; used to send death threat; inappropriate arrest
- important individuals involved-president; number of individuals involved-entire faculty; police involved; threat of violence made

Rating: 4
Rationales:
- death threat makes this an extremely serious incident, perhaps not for IT department, but for institution. Un-moderated faculty-wide mailing list also serious problem for the institution. Misuse of another student’s password also very serious, but little IT can do about that other than work within college judicial system
- criminal activities
- illegal act; distribution of email and public knowledge
- death threat bumps this up to the highest level of urgency
- not so serious an offense from a University perspective but for Matt it is very serious with career and life
- explicitness of message, potential criminal charges, these make this incident much more serious
- death threat, police, FBI involvement
- identity theft, threatening someone via use of university network
- death threat and gory details; stolen password and consequences of the incident; arrest of innocent party
- violated computer use policies; impersonated someone else; threatened the president—potential crimes
- hijacking of an account to send a death threat
- pw on a sticky note; message to president; faculty-wide mailing list un-moderated
- death threat is a felony crime
- Pw on a sticky note
- nothing more serious than a threat to life or physical safety
- violates several items of AUP; wrongful use of computer resources; wrongful use of ID and pw; harassment
- police arresting the student without apparent investigation; death threat
Incident 4: SO CLOSE YET SO FAR

Bill and Ted are network security officers at a small liberal arts college in Iowa. They regularly check their IDS and firewall logs to see what has been happening. One Monday they discover that there has been a dozen attempts to log into the root account on the administrative file server over the weekend. Each time, the first six letters of the password (the password was “pencil”) were correct but the hacker kept adding an ampersand to the end. Bill and Ted examined the logs and traced the IP address to an ISP in San Antonio. Police obtain a subpoena for the name of the account holder, track down and confiscate the equipment and charge the suspect. Meanwhile, Bill and Ted try to find out how the hacker knew the password. They find than an IRC zombie has been installed on a faculty member’s computer, and that this bot was recording everything sent over the network in clear text that looked like a login screen. Rather than logging in using SSH, the root administrator had been using Telnet, thus making the password as sniffable as a new car.

Rating: 1 N/A

Rationales:
- attempts to break into University network
- attempted login was not successful, so network remains secured
- root administrators insecure process
- no crime or damage
- use of telnet rather than SSH; IRC bot

Rating: 2

Rationales:
- use of telnet rather than SSH is a very serious mistake for people who are responsible for network security.
- root administrator for central system using completely insecure methods to access a privileged account from a machine of unknown integrity
- lapse of judgment in using Telnet-serious enough because of the position of these two individuals.
- hacking an administrative server; IRC zombie installed on a faculty machine
- systemic vulnerability
- lack of system security; use of a dictionary word as the root password, and apparent lack of monitoring tools to detect spyware, etc. Although the perpetrator of the hack was clearly at fault, the network security officers are equally liable.
- multiple login attempts with an almost completely un/password; attempt against administrative file server
- bot recording everything sent over network in clear text; six letter password on root account; root administrator using Telnet—all indications that security is in a shambles and must be fixed.
- Password needs to be tougher; Confidential information should be encrypted and application secured
- use of Telnet
- boot administrator using clear text; zombie installed on univ computer for purpose of gathering ID & pws
- could expose university to considerable damage (cost of notification) and loss of prestige

Rating: 3

Rationales:
- machine compromise. Attempted compromise of administrative file server.
- root account administrative server-loss of disclosure of data—both FERPA and long-term ID theft issues.
- no password complexity rules, logging text of failed passwords, allowing telnet access to a critical server, using root account at all over the net instead of pseudo;
- root administrator was using such a simple password that he had been communicating it in clear text.
- machines and networks not adequately protected; multiple unsuccessful attempts did not create an alarm;
- lack of encrypted transmission
- correct insecure procedures by system administrators and architectures that mingle acad. and adm. traffic.
- bot recording everything sent out over the network; root administrator has been using Telnet
- extremely serious due to the potential for loss and/or compromising of extremely sensitive information.
- root administrators use of clear text protocol; sniffing has been successful; probable arrest of innocent party

Rating: 4

Rationales:
- root account administrative server-loss of disclosure of data—both FERPA and long-term ID theft issues.
- no password complexity rules, logging text of failed passwords, allowing telnet access to a critical server, using root account at all over the net instead of pseudo;
- root administrator was using such a simple password that he had been communicating it in clear text.
- machines and networks not adequately protected; multiple unsuccessful attempts did not create an alarm;
- lack of encrypted transmission
- correct insecure procedures by system administrators and architectures that mingle acad. and adm. traffic.
- bot recording everything sent out over the network; root administrator has been using Telnet
- extremely serious due to the potential for loss and/or compromising of extremely sensitive information.
- root administrators use of clear text protocol; sniffing has been successful; probable arrest of innocent party