

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

**VOLUME II: CORPORATE AND NOT-FOR-PROFIT
SAMPLE**

Virginia E. Rezmierski, Ph.D.
Mark A. Bard, MSI
Brady T. West, MA, BS

This work was made possible through funding from the National Science Foundation. 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 or the University of Michigan.

© 2006 The Regents of the University of Michigan. Some 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.

Table of Contents

<i>Executive Summary</i>	<i>ii</i>
<i>Acknowledgements</i>	<i>iv</i>
I. Introduction and Background	1
II. Study Preperation	2
III. Data Collection and Management	4
IV. Univariate Analysis and Sample Comparison	6
V. Cause & Prevention Factors and Best Practices	18
VI. Conclusions and Recommendations	30
Appendices	
A: CIFAC Instrument	36
B: Sample of CIFAC Incidents	42
C: Frequency Tables for Differences Between Samples	44
D: Variable Clusters for Each Factor	48
E: Best Practice Scoring Scales	56

Executive Summary

The Computer Incident Factor Analysis and Categorization (CIFAC) project received supplemental support from the National Science Foundation in late 2005, making it possible to expand the scope of the project to include data collection from Corporate and Not-for-Profit participants. Already in 2005, the CIFAC project team had completed collection and analysis of data regarding computer-related incidents that occurred within Academic environments.

The Final Report –Volume I: College and University Sample was completed in 2005. This Final Report--Volume II: Corporate and Not-For-Profit Sample, provides information about the results from analysis of the second sample, as well as comparisons of results from the two CIFAC samples.

Under support and guidance from a selected and distinguished National Advisory Board, researchers collected data regarding computer-related incidents using a standardized survey instrument and an “in-person” interview methodology. “Incident” was defined broadly in the CIFAC study, to avoid a too narrow focus on technical aspects of incidents.

The CIFAC survey questions encompassed 81 variables regarding the cause of incidents and what it would take to prevent the incidents from happening. Respondents rated the seriousness of the incidents, categorized each incident according to its focus—people, systems, or data—and provided detailed information about recommended best practices for preventing, mitigating and managing the incidents. Respondents also provided information regarding incident handling and management procedures and the organizational and management structure of their IT organizations.

In the Corporate/NFP sample, researchers gathered 110 incidents from 28 organizations. A balanced sample, based upon organization size, type (Corporate v. NFP) and focus, was obtained. Approximately 1% of incidents reported by the Corporate/NFP participants were identified as “not at all serious,” 23% were identified as “somewhat serious,” 37% “quite serious,” and 39% as “extremely serious.”

Analysis of the study data showed that the respondents in the two samples (Academic and Corporate/NFP) responded very similarly in response to the cause and prevention questions. Only 19 of the 81 variables had significantly different responses between the samples. These differences were generally explained due to differences in organizational and management structures within academia and the corporate environments.

Researchers completed a factor analysis to determine if certain variables cluster together in order to explain the variability in responses from participants. Names were assigned to these factors based upon the variables that clustered together within them. In the Academic sample, 6 cause factors explained 57.3% of the variability and 6 prevention factors were identified to explain 54.6% of the variability. Eight cause factors explain 66.6% of the variability and 8 prevention variables explain 66.5% of the variability within the Corporate/Not-for-Profit sample. An analysis of variance (ANOVA) was conducted to determine which factors are important in the cause and prevention of serious incidents and incident types.

As a cause of computer-related incidents, researchers concluded that for both of the CIFAC study samples, lack or deficiency of training/education played an important role in causing computer incidents. Training/education and requirements for IT managers and staff and for non IT staff members is an important-- perhaps critical-- process to be addressed to eliminate the cause of many of the systems and data incidents, as well as the most serious of the incidents that are occurring. To prevent computer-related incidents from happening, researchers found, for both of the CIFAC study samples, that increased management procedures and increased access control requirements would play an important role. Again, increased training/education for non-IT staff and for external users was seen as a necessary measure for preventing computer-related incidents. In the Academic sample, increased hardware, software and personnel resources were also felt to be related to preventing the most serious systems incidents from occurring. Corporate respondents saw increased access control requirements and management procedures for detection, response and recovery as most important in addressing the most serious of the computer-related incidents. Addressing the need for increased management procedures and access control could prevent the extremely serious incidents from occurring.

As part of the data collection, researchers asked participants to share a best practice to prevent, mitigate and manage an incident. The responses were then scored into a category based upon the responses given. From these scores, raw frequencies were tabulated to determine the most recommended best practices for prevention, mitigation and management. Further, Wald chi-square tests were used to determine if there were associations between certain best practices and the focus of the incident, the seriousness of the incident or the sample (Academic or Corporate/NFP) from which they came. Wald chi-square tests indicated that incident focus, incident seriousness, and sample were all significant predictors of recommended best practices.

Given the results of this CIFAC study, researchers provided recommendations for Academic, Corporate and Not-for-Profit organizations to help prevent the occurrence of computer-related incidents and to encourage the practice of recommended good practice in computing services.

Acknowledgements

The staff of the CIFAC project acknowledges the considerable contributions made by organizations and individuals in support of this project. These organizations shared their time, expertise, information and insights regarding computer-related incidents.

We are especially thankful for the time and expertise shared by Chief Information Officers, information technology staff, risk managers, human resource and information security officers of the twenty-eight corporations and not-for-profit organizations that participated in this segment of the CIFAC study. These individuals arranged meetings and spent time sharing information regarding incidents that had occurred within their organizations. They welcomed the opportunity to discuss these incidents and were tolerant of the many questions necessitated by the research. Without their willing participation, this study could not have been accomplished.

We acknowledge and thank the Division of Information and Intelligent Systems within the National Science Foundation for its support and for the supplemental funding which made data collection in this segment of the study possible. The people-intensive methodology of this study and the protectiveness of the Corporate environment made it necessary for the research team to spend considerable time developing relationships in order to gain access to the data. The additional support from NSF made this Segment II of the CIFAC study possible.

The Advisory Board of the CIFAC project was again instrumental in providing support and guidance to Segment II of the study. After the completion of Segment I-the College and University sample, members of the Board were invited to continue their service through the second part of the study- Segment II. While this meant an additional time commitment of approximately one year on each of their parts, we were delighted that each member of the Board agreed to continue their participation. They have been particularly instrumental in assisting and guiding the research team for the dissemination of study results.

The research team is especially thankful for the expertise of Mr. Brady West of the University of Michigan's Center for Statistical Consultation and Research. Mr. West provided expert consultation and statistical analysis for this project, helping to guide our inquiry into the data and our interpretation of results. His patience and skill are very much appreciated.

A special thank you is extended to Mr. Dan Rothschild of George Mason University's Mercatus Center. Mr. Rothschild was a staff member for Segment I of the CIFAC study and provided invaluable assistance during the analysis of the best practices.

Several administrative staff of the University of Michigan also contributed to the completion of this study. Ms. Lori Coleman, in conjunction with the project director, provided financial management and monitoring of the project. Ms. Sharon Disney, Ms. Carrie Gardner and Ms. Jill Crane provided administrative support managing travel and logistics. We are thankful for the professional processes and skills of these administrators.

The administrative, statistical, and advisory support and expertise that surrounded this project, from the beginning of the CIFAC Segment I-College and University Sample, through the completion of Segment II-the Corporate and Not-for-Profit Sample, made it possible for the research team to concentrate on the study itself-collection of the data and interpretation of the results and allowed us to complete the study in a professional and timely fashion.

I. Introduction and Background

A. Introduction

This report, Volume II of the CIFAC study, contains the information pertaining to the second segment of the CIFAC study. Final Report -Volume I, described the project pertaining to the first sample of the CIFAC study—the college and university sample.¹ This Report-Volume II, describes the project pertaining to sample II—the Corporate and not-for-profit, hereafter referred to as NFP, sample. It also describes the way in which the two segments of the CIFAC project relate, are alike or are different. Volume II also provides the synthesis of conclusions and recommendations for the full CIFAC study.

B. Background

Prior to the beginning of the CIFAC 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 the field. The review of literature appears in Volume I of this study.

The literature review allowed us to draw conclusions regarding the definition of an incident, regarding taxonomies and categorizations, and regarding the need for metrics. That review, coupled with input from professional focus groups and our own previous experience, determined the design of the CIFAC project. There is a focus on incident categorization, a broad definition of computer-related incidents, analysis perceived seriousness, and analysis of factors relating to the cause and prevention of incidents. The review resulted in the authors collecting data regarding three categories of incidents—those focused on people, on data, and on systems. It also resulted in the collection of ratings of incident seriousness, on a scale of: “not at all, somewhat, quite, and extremely.”

The study design and implementation were consistent for both segments. The CIFAC project was designed to collect and analyze data regarding factors relating to cause and prevention of different types of incidents from a large data set collected from colleges, universities, corporations and NFP organizations.

The CIFAC study 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 managers, 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 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.

¹ Final Report-Volume I is available at <http://www.educause.edu/LibraryDetailPage/666?ID=CSD4207>

II. Study Preparation

In preparing for the 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 robust data collection instrument. The data collection instrument is discussed in Section III Data Collection and Management.

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 managers, 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	Associate Vice President for Telecommunications, Indiana University
Robert N. Clark, Jr.	Director of Internal Audit, Georgia Institute of Technology
E. Eugene Schultz	Chief Technology Officer, High Tower Software
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 Board served faithfully through the implementation of Segment I of the study, meeting together and also discussing implementation and results via telephone conferences. When asked to serve for Segment II of the study, each member again enthusiastically agreed. They have provided invaluable feedback, criticism, suggestions, ideas, and support to the research staff. They have also facilitated dissemination of the study results to the organizations they represent and to other professional groups.

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. In Segment I of this study, due to some limitations on travel funds, researchers selected different geographic areas with sufficient numbers of large, small, public and private colleges and universities to provide some general geographic distribution for the study sample. They then contacted Chief Information Officers in each of the targeted schools and invited their participation in the study. Within academia, researchers had credibility and an established professional network. Hence, the reception for research of this type, though computer incident data are considered sensitive and protected, was generally positive and inviting.

For Segment II of this study-Corporate and NFP- however, project travel funds were even more restricted. The research team did not have as much credibility within the Corporate/NFP sector, as compared to the Academic. Further, researchers did not have established professional networks in the Corporate and NFP sector. Data regarding computer incidents were viewed as extremely sensitive and information about the incidents enjoyed even greater protections. Therefore, access for Segment II was more difficult to obtain.

In the CIFAC National Science Foundation grant proposal, referring to the difference in privacy expectations between College and Corporate populations, the Principal Investigator wrote:

This dynamic (lack of trust) may create a sense of tension therefore between researchers from academia doing research with 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.²

This proved to be the case. Therefore, researchers decided to cast a wide net of inquiries to obtain the names of key executives from any organization within a restricted travel area of the Midwest--Michigan, Ohio, and Illinois. Regardless of the type of organization, if key contact information for an executive was obtained, that organization was viewed as a potential participant. Researchers also broadcast an invitation to participate through professional computer security groups. In this process, an effort was made to specifically recruit organizations with large and small user populations and to balance the sample with approximately equal numbers of participating corporations and NFPs.

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 critical 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.

In the time allotted for Segment II development, the research team was able to identify 28 Corporations and NFP organizations interested in participating in the CIFAC study. A couple of these self-selected, having heard about the study from other organizations. While the initial recruitment proved very difficult, researchers found that once the study was understood and the personal contacts were begun, individuals became willing to recommend the study to others and recruitment of a participant pool became easier. Though there was an initial goal of 30 organizations, the sample was closed at 28 to meet the timeline set for the project.

The method of communicating with participating organizations was the same for Segment I and II participants. Researchers personally contacted the Chief Information Officer or Vice President in charge of Information Technology at each organization. For many of the NFPs, the person in charge was the system administrator or financial administrator. The contact person was told about the CIFAC project. They were informed of obligations associated with participation and asked to identify up to three people within their organization to serve as participants in the study.

Specifically, the high-level contact was 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." These participants were expected to be professionals who were well-versed in the problems causing these incidents and the handling of the incidents, and were expected to be capable of providing detailed data and best practices relative to each reported incident. The contacts were asked to personally inform selected participants that they were authorized to meet with the CIFAC research team. The participants were expected to provide data regarding three incidents that occurred within the previous 12-18 months.

From this point, the research team had direct contact with each of the identified participants for scheduling and data collection. Data collection was conducted by members of the research team in-person, on site, at each of the participating corporations or NFP organization. Incident data were collected between October 2005 and January 2006. For three of the participants who had self-selected and for whom distance prohibited in-person data collection, data were collected over the telephone. Once direct contacts had been established with designated representatives from the participating organizations, researchers received a warm reception and outstanding cooperation. Further, participants in the study began to refer us to other individuals in their professional network to the project.

² Rezmierski, V (2003). "CIFAC: Computer Incident Factor Analysis and Categorization Project", IIS-Digital Society & Technologies Grant Proposal DUNS#073133571, 9.

III. Data Collection and Management

The data collection methodology is discussed in this section of the report. Information is also provided regarding the management of data in Segment II of this project.

A. Data Collection Instrument

The same instrument used in Segment I of the CIFAC study was used in Segment II. (The full instrument appears in Appendix A of this report.) The instrument contained 34 questions representing approximately 125 variables that were designed to collect information about incidents including: type, perceived seriousness, factors that could have prevented the incidents, factors that caused the incident, factors that affected the speed and manner of reaction to an incident, and procedural questions. The instrument focused entirely on the incident being reported, and each participant responded to the same set of questions on the instrument for up to three incidents. No personal information about their employment histories, qualifications, or specific work responsibilities. A commonly employed opinion category quantifier of four possible responses was used, throughout the instrument. The foils for the Likert scale were “not at all”, “somewhat”, “quite”, and “extremely.”

The definition of computer-related incident that was used throughout this study was as follows:

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.

This definition was read to each respondent. The respondents then selected and described an incident to report (a sample of incidents appears in Appendix B of this report). For each incident, respondents were asked to judge the seriousness of the incident on the four point scale above. After rating the seriousness of the incident, respondents were asked to explain why they had selected that rating. They were then asked to identify the primary focus—data, people, or systems—of the incident.

Next, respondents were asked a series of questions with 36 items/variables related to prevention. They were asked to rate each variable, using the scale detailed above, on its importance in preventing the incident. These questions fell into 7 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, customer/clients, 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. Existence of 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 required of customer/clients, non-IT staff, and authorized external users prior to use of systems; and
7. Improved configuration for networks, desktop software, desktop hardware, server or mainframe hardware, and server or mainframe software.

Following the prevention questions, the respondents were asked to rate the importance of 45 variables on a parallel series of 7 questions relating to the cause of the incident plus two additional questions regarding behavior:

1. Accidental or careless behavior of IT managers, IT staff, non-IT staff, customers/clients, authorized external users, and unauthorized external users;
2. Malicious or abusive behaviors of IT managers, IT staff, non-IT staff, customers/clients, authorized external users, and unauthorized external users.

Data were collected on the adequacy and effectiveness of their organization's pre-established incident response procedures. Respondents were asked what stimulated them to act in response to an incident. Finally, the instrument gave each respondent an opportunity to identify and share with colleagues a best practice for prevention, mitigation and management of the incident.

B. Data Management

As was done in Segment I of this study, data were collected in-person from the respondents and entered on a laptop computer using SPSS Data Entry 4.0 software. Researchers placed the data directly from the laptop files into the data analysis SPSS files. Once data were reviewed for errors, the backup copies were destroyed. Because the SPSS Data Entry tool allows the survey responses to be pre-coded as numeric, the data transfer to the analysis program eliminated data entry errors.

Care was taken to eliminate all of the organizational and respondent identifiers connected with the data. Because of the sensitivity assigned to incident data by Corporate and NFP organizations and the restricted geographic area from which participating organizations have come, the names of participating organizations are not included in the appendix of this report, unlike the final report from college and university participants.

IV. Univariate Analysis and Sample Comparisons

Analysis and findings of the CIFAC study Corporate/NFP data will be described in three sections. Section A provides a general description of the make-up of the sample. Section B provides a description of how participants responded to the cause and prevention variables in the study. Section C provides discussion and analysis of how the results from the two samples, the college and university and those of the Corporate and NFP, compare and differ.

A. General Sample Description

As was described in the Data Collection and Management section of this report, it was difficult to gain permission to collect data from the Corporate and NFP organizations. Most personnel from NFPs that deal with sensitive data are hesitant to share information regarding their processes, systems, or data management practices for fear that member privacy will be violated. Likewise, Corporate organizations are hesitant to share information regarding computer incidents for fear that any release of such information could erode the public's and shareholder's trust in the organization, and possibly affect the company's bottom line--profit.

Aware of this difficulty, the research team decided to be rather random in our search for participating organizations. The goal was to collect data from 30 Corporate/NFP organizations, approximately half from corporations and half from NFP agencies. While we were cognizant of the need for large and small organizations in each segment of the sample, we did not reject any organization that expressed an interest in participating. Instead, researchers tried to sufficiently develop relationships so they could add organizations to balance the sample, if needed. Researchers were surprised that even though the sample selection was not statistically random, was geographically-based for the most part, and was identified based on willingness to participate, the resulting distribution of organizations by size and type was remarkably balanced.

The charts below show, relative to organizational size, 7 corporations with less than 5000 users and 6 with more than 5000. There were 6 NFP organizations with less than 5000 users and 9 with more than 5000. The total number of corporations in Sample II was 13; the total number of NFPs in this sample was 15.

Participating Organizations

	Corp	NFP
< 5000 users	7	6
> 5000 users	6	9

Due to time constraints, we terminated data collection with 28 participating organizations in Sample II. Within these organizations, 42 people participated, yielding data on 110 incidents. Combining the Academic and the Corporate/NFP samples, the total study involved 64 organizations, 134 participants, and yielded data regarding 430 computer related incidents.

Sample Description

	Academic	Corporate/NFP	Total
Number of Sites	36	28	64
Number of Participants	92	42	134
Number of Incidents	320	110	430

The two samples were very nearly identical in the distribution of seriousness ratings for the incidents they provided. Approximately 1% of incidents reported by the Corporate/NFP participants were identified as "not at all serious," 23% were identified as "somewhat serious," 37% "quite serious," and 39% as "extremely serious." Comparable distribution was seen in the Academic sample, where College and University respondents

identified, 2% “not at all,” 26% “somewhat,” 31% quite,” and 41% “extremely serious.” It should be noted that a low response rate for the “not at all” category of seriousness is not surprising since respondents were free to select the incidents they reported, from those occurring in the previous 12-18 months. Researchers believe that respondents selected the most serious incidents and less mundane incidents to report.

Incident Seriousness

Seriousness	Not At All	Somewhat	Quite	Extremely	Total*
CNFP	1	25	40	43	109
% within Sample	0.92%	22.94%	36.70%	39.45%	100.00%
Acad	7	82	99	132	320
% within Sample	2.19%	25.63%	30.94%	41.25%	100.00%
Combined	8	107	139	175	429
% within Sample	1.86%	24.94%	32.40%	40.79%	100.00%

Similarity existed in the categorization of incidents between participants in the two CIFAC samples as well. Slightly more of the Corporate and NFP participants categorized their reported incidents as “people” incidents than did the college and university participants. Slightly more of the Academic participants categorized their reported incidents as “systems” incidents. However, the general distribution of reported incidents between the three categories, people, data, and systems, was comparable between the two samples.

Incident Type

Focus	People	Data	Systems	Total*
CNFP	43	24	42	109
% within Sample	39.45%	22.02%	38.53%	100.00%
Academic	93	84	140	317
% within Sample	29.34%	26.50%	44.16%	100.00%
Combined	136	108	182	426
% within Sample	31.92%	25.35%	42.72%	100.00%

* The total number of incidents in the study was 430. One respondent did not rate seriousness, thus the combined N=429 above. Likewise four respondents did not rate focus of the incident to yield N=426 above.

B. Responses to Cause and Prevention Questions

How did participants in Sample II respond to the study questions regarding the cause of incidents?

Univariate analysis was performed on the 81 variables within the CIFAC study’s seven prevention questions and the nine cause questions. The entire set of study questions appears in Appendix A of this report. For example, respondents were asked:

“To PREVENT this incident from happening in the future, how important is increasing the availability of the following RESOURCES: personnel, hardware, software networks, physical security, and access control tools.”

Respondents rated the importance of each of the 36 prevention variables on a scale selecting from 1-4: “not at all,” “somewhat,” “quite,” and “extremely.” The prevention questions queried the importance of increasing various types of resources, training/education, procedures, and processes such as logging, performance requirements, knowledge levels and configuration requirements.

1. Results from Prevention Questions

What did the Corporate/NFP respondents perceive as important in preventing incidents?

In general, it appeared that additional resources were not seen as needed for prevention of computer-related incidents, with the exception of access control tools. Details include:

- Respondents felt that for 61% of the reported incidents, increasing the availability of access control resources was “somewhat, quite or extremely important.”
- Increasing the availability of personnel resources was perceived as less important in preventing incidents from occurring. Eighty-four (84%) said “not at all or somewhat important.” Only 2% said increased personnel resources would have been extremely important in preventing the incidents reported.
- Increasing hardware resources was not perceived to be an important prevention variable. 66% of the incidents it were rated “not at all important.”
- Increasing software resources was not perceived to be an important prevention variable. Respondents indicated 68% of the cases were rated “not at all or somewhat important.”
- Respondents attributed little importance to additional network resources as prevention for 85% of the incidents.
- Likewise, added physical security resources were not seen to be important in 89% of the incidents reported.

When queried about the importance of education, respondents attributed more importance to the education variable. Specifically, responses indicate that increasing education for IT management and IT staff is important to prevent incidents from happening in the future.

- Education of external users was not felt to be very important as a prevention for future incidents.
- Increased education for IT managers was felt to be “somewhat, quite, or extremely important” in preventing 72% of the incidents, with 37% rated as “quite or extremely important” for prevention of the incidents.
- Increased education for IT staff members was seen as “somewhat, quite or extremely important” for 78% of incidents; rated as “quite or extremely important” for prevention in 44% of incidents.
- Increased education for non-IT staff as a prevention of computer-related incidents was rated “somewhat, quite or extremely important” for 61% of the incidents.

With the exception of increased procedures for detecting and patching software bugs, respondents indicated that additional procedures are not important for prevention..

- Increased procedures for detecting software bugs as a prevention of incidents was rated “not at all or only somewhat important” for 71% of incidents.
- Likewise, increased procedures for network management were not felt to be particularly important in preventing incidents. They were rated “not at all or somewhat important” for 65% of the incidents. For 36% of the cases, however, increased procedures for network management were felt to be “quite or extremely important”
- “Not at all or somewhat important” was the response to increased procedures for backup and disaster recovery for prevention for incidents. This was the response for 79% of incidents. This unimportance in preventing incidents could be explained due to perception of backup as a recovery process rather than a prevention process.

- Increasing procedures for documenting systems was seen as a slightly more important variable in preventing incidents. It was rated “quite or extremely important” for approximately one third, 31%, of incidents.
- Increasing procedures for audit was seen as “not at all or only somewhat important” for 56% of the incidents in. Respondents felt that increasing such procedures was “not at all important” for 24% of these incidents.
- Increasing procedures for detecting software flaws was felt to be “somewhat, quite, or extremely important” for 67% of incidents.

The existence of documentation, policy, and logging were seen as important in preventing incidents from happening.

- The existence of documentation was generally felt to be “not at all or only somewhat important” for 66% of incidents. Generally the use of documentation is important in the recovery process once an incident has occurred, perhaps less so in the prevention of incidents.
- The existence of policy was rated as “quite or extremely important” for preventing 50% of the incidents reported
- The existence of logging was felt to be “somewhat, quite or extremely important” for preventing 76% of the Corporate/NFP sample of incidents; it was “extremely important” for preventing 17% of cases. Analysis of logs was rated “quite or extremely important” for preventing 53% of incidents.

When asked about the importance of increasing requirements, respondents indicated that improving configuration requirements for mainframes and servers and networks was important. Other variables, including requirements for the handling of personal information, increased requirements for IT managers and staff and requirements for the configuration of desktop software were important less often.

- Increasing requirements for the handling of personal information as a prevention measure was felt to be “not at all important” for 69% of the incidents. Some participants indicated that such requirements were already in place.
- Respondents indicated having increasing requirements for IT staff was “not at all or only somewhat important” in preventing incidents from happening for 70% of the reported incidents. Further, having increased requirements for IT managers was “not at all or only somewhat important” as a prevention for computer related incidents.
- Respondents felt that improving configuration requirements for mainframes and servers was “not at all important” in 27% of incidents, but was “somewhat, quite or extremely important” in 73% of their reported incidents.
- Improving configuration requirements for networks was rated “not at all important” for preventing 35% of the reported incidents but “somewhat, quite, or extremely important” for 66% of the incidents
- Improving configuration requirements for desktop software as rated “quite or extremely important” for 20% of reported incidents. It was rated as “not at all important” for 60% of incidents.

Regarding prevention, Corporate/NFP respondents felt that the most important variables for preventing incidents were increasing education for IT managers and IT staff, increased procedures for detecting and patching software flaws, increasing procedures for logging, and increasing configuration requirements for mainframes and servers.

2. Results from Cause questions

What did respondents in the Corporate/NFP perceive as the cause the incidents?

Respondents were asked a set of cause questions that closely followed the pattern of the previously asked prevention questions. For example:

“In CAUSING this incident to happen, how important was the lack or deficiency of the following RESOURCES: personnel, hardware, software, network physical security?”

Two additional questions were added to the CAUSE questions to query the importance of accidental/careless and/or abusive/malicious behavior.

“In CAUSING this incident to happen, how important was ACCIDENTAL or CARELESS behavior of: IT managers, IT staff, non-IT staff, clients/customers, authorized or permitted external users, and unauthorized external users?”

“In CAUSING this incident to happen, how important was MALICIOUS or ABUSIVE behavior of: IT managers, IT staff, non-IT staff, clients/customers, authorized or permitted external users, unauthorized external users?”

For most of the questions querying the importance of a lack of various types of resources as the cause of the incidents, respondents in Corporate/NFP rated the items as very low in importance in causing the incidents. Regarding a lack of resources then, respondents generally did not feel that resources were the primary cause of incidents. Of all the resource variables, lack of personnel was seen as quite or extremely important for 20% of incidents and lack of software resources, “quite or extremely important” for 26%. Here is a breakdown by variable:

- Regarding lack of physical security resources as the cause, respondents said “not at all important” for 81% of the incidents.
- Lack of personnel resources respondents was rated “not at all or somewhat important” for 80% of the incidents. However, for 20% of the incidents, a lack of personnel resources was “quite or extremely important.”
- Regarding a lack of hardware resources respondents said “not at all important” for 80% of incidents.
- Lack of software resources was seen as a bit more important however, with 73% saying “not at all or somewhat important”. A lack of software resources was rated “quite or extremely” important as the cause in 26% of the incidents.
- A lack of network resources was seen as much less important as a cause for 89% of the incidents.

For the questions querying the importance of a lack of education and training as the cause of incidents, respondents were more varied in their answers. In approximately one quarter of the reported cases, a lack of education/training for some employee was seen as “quite or extremely important” in causing the incident. Below are the details:

- A lack of education/training for IT managers was scored as “quite or extremely important” as the cause of 21% of incidents.
- A lack of education/training for IT staff was felt to be “quite or extremely important” as the cause of 27% of the incidents reported.

- A lack of education/training for non-IT staff was rated as “quite or extremely important” as the cause of 26% of incidents.
- A lack of education/training for incident investigators was not felt to be important as the cause, “not at all or somewhat”, for 82% of cases.

Regarding the lack or deficiency of procedures for various tasks, respondents in Sample II felt that such a lack was generally “not at all or only somewhat important” as the cause of the incident.

- Lack or deficiency of procedures for auditing systems—“not at all or somewhat important” for 72%, however “quite or extremely important” for 28% of incidents.
- Lack or deficiency of procedures for network management-- “Not at all or somewhat important for 78% of incidents, however “quite or extremely important” for 22% of incidents.
- Lack or deficiency of procedures for incident response—“not at all or somewhat important” for 81% of incidents, however “quite or extremely important” for 19%.
- Lack or deficiency of procedures for backup and disaster recovery—“not at all or somewhat important” for 82% however, “quite or extremely important” for 11% of incidents.
- Lack or deficiency of procedures for documenting systems and networks—“not at all or somewhat important” for 81%, however, “quite or extremely important” for 19% of incidents.

As a cause of computer-related incidents, respondents identified a lack of procedures, especially auditing procedures, as “quite or extremely” important in 11% to 28% of incidents.

When queried about the importance of a lack or deficiency in performance and operational requirements as the cause of incidents, respondents indicated that most were “not at all important” as the cause of the incidents. However, again, as in the previous items, there are a consistent percentage of incidents for which the variables are scored “quite or extremely” important as the cause.

- Lack of or deficiency in requirements for the handling of personal information— “not at all important” for 83% and “somewhat, quite, or extremely important” in 17% of incidents.
- Lack or deficiency in requirements for IT managers—“not at all important” for 63% and “somewhat important” for 29% of incidents.
- Lack or deficiency in requirements for IT staff—“not at all important” for 59% of incidents, and “somewhat, quite, or extremely important” for 41% of incidents.
- Lack or deficiency in requirements for non-IT staff—“not at all important” for 68% of incidents, and “somewhat, quite, or extremely important for 32% of incidents.
- Lack or deficiency in requirements for the use of institutional resources—“not at all important” for 46% of the incidents, and “somewhat, quite, or extremely important for 54% of incidents.

Regarding the deficiency in requirements, respondents in Sample II indicated that such a deficiency or lack played a role in causing the incidents, ranging from 17% to 54% depending on the requirements being considered.

For the most part, respondents did not feel that the level of knowledge required prior to using systems for was an important variable in causing computer-related incidents for their authorized external users. For 94% of the incidents, respondents indicated that it was “not at all or only somewhat important.”

Respondents were asked to consider and rate the importance of a lack or deficiency in configuration requirements as the cause of computer-related incidents.

- Lack or deficiency in configuration requirements of mainframe and server software—Respondents indicated that for 59% of the incidents, this variable was “somewhat, quite or extremely important” as a cause. In fact, it was “quite or extremely important for 21% of incidents.
- Lack or deficiency in configuration requirements for networks—Respondents indicated that for 46% of incidents it was somewhat, quite, or extremely important in causing the incident. For most of the incidents (54%), however, it was “not at all important”.
- Lack or deficiency in configuration requirements for desktop software—Respondents indicated that this variable was “not at all or only somewhat important” as a cause in 85% of the incidents.
- Lack or deficiency in configuration requirements for desktop hardware—Respondents were very strong in indicating that this variable was “not at all important” in causing incidents in 96% of the incidents.
- Lack or deficiency in configuration requirements for mainframe or server hardware—Respondents indicated that for 92% of the incidents, this variable was “not at all or only somewhat important” as a cause of the incident.

Regarding configuration requirements, Corporate/NFP respondents indicated that lack or deficiency in configuration requirements for mainframe and server software and networks caused a percentage of the incidents. This will be discussed in more detail later in this report as we examine the differences between participant responses in the two samples and the differences in the work environments represented.

Lack of management processes were queried via six additional questions. Respondents concluded that of the processes variables, only a lack in promulgation of documentation and policies had a strong relationship to cause of incidents. Here is a summary of responses:

- Lack or deficiency in identification, authentication and authorization processes—In 41% of the incidents, this variable was “somewhat, quite or extremely important” as a cause; for 24% it was rated as “quite or extremely important.”
- Lack or deficiency in backup and recovery processes—Respondents strongly rated this variable as “not at all important” in causing incidents for 92% of the incidents reported. It should be noted that backup and recovery is generally considered part of recovery processes rather than the cause of incidents.
- Lack or deficiency in documentation of systems—For 84% of incidents, respondents scored this variable as “not at all or somewhat important” in causing the incident.
- Lack or deficiency in promulgation of documentation and policies—For this variable, respondents indicated that for 56% of the incidents, it was “somewhat, quite, or extremely important” in causing the incident. Of those, it was felt to be “quite or extremely important” for 31% of the incidents.
- Lack or deficiency in logging—Respondents indicated that for 86% of incidents, this variable was “not at all or somewhat important” as a cause.
- Lack or deficiency in analysis of logs—Respondents felt that for 49% of incidents, this was “somewhat, quite or extremely important” as a cause.

3. Results Regarding Malicious and Accidental Behavior Questions
How important did respondents think malicious or accidental behaviors of various people were in causing the reported incidents?

Finally, researchers asked Corporate/NFP participants to answer questions about the accidental or careless behaviors of several different groups of people, and about the importance of abusive or malicious behaviors of the same groups of people in causing incidents. Two additional questions were added to the cause questions to query the importance of accidental/careless and/or abusive/malicious behavior.

“In CAUSING this incident to happen, how important was ACCIDENTAL or CARELESS behavior of: IT managers, IT staff, non-IT staff, clients/customers, authorized or permitted external users, and unauthorized external users?”

“In CAUSING this incident to happen, how important was MALICIOUS or ABUSIVE behavior of: IT managers, IT staff, non-IT staff, clients/customers, authorized or permitted external users, unauthorized external users?”

Regarding careless or accidental behaviors as the cause of incidents, respondents indicated that for IT managers, IT staff, and non-IT staff such behaviors contributed to, or were the perceived cause of, 30-40% of the incidents. Regarding malicious or abusive behaviors as the cause of incidents, respondents indicated that the largest percentage of incidents caused by this kind of behavior came from unauthorized external users (33%), but that IT managers, IT staff, and non-IT staff, while generally not the cause of incidents, were responsible through malicious or abusive behavior for approximately 15-17% of incidents. The details are below:

- Accidental or careless behaviors of IT managers—For 35% of incidents, respondents felt that accidental or careless behavior of IT managers was “somewhat, quite, or extremely important” in causing the incident. It was “quite or extremely important” in 17% of these incidents.
- Accidental or careless behaviors of IT staff—For 39% of incidents, “somewhat, quite, or extremely important” in causing the incident; “quite important” in 17% of these incidents.
- Accidental or careless behaviors of non-IT staff—For 35% of incidents, “somewhat, quite, or extremely important” in causing the incident; “extremely important” in 15% of incidents.
- Accidental or careless behaviors of authorized external users—Respondents were strong in indicating that for 84% of incidents, this variable was “not at all important.”
- Malicious or abusive behavior of unauthorized external users--“quite or extremely important” as a cause in 33% of incidents.
- Malicious or abusive behavior of IT managers—For the most part, respondents said that this was “not at all important” as a cause of incidents (97%). It is important to note, however, that for 3% of the incidents, it was rated as “quite important.”
- Malicious or abusive behavior of IT staff—Again, respondents indicated that this was “not at all important” in causing the incident for a large percentage of the incidents (93%). However, again, it is important to note that for 8% of the incidents it was “quite or extremely important.”
- Malicious or abusive behavior of non IT staff—“Not at all important” for 85% of cases, but for 13%, “quite or extremely important” as the cause.
- Malicious or abusive behavior of authorized external users—Respondents strongly indicated that this variable was “not at all important” for 96% of the incidents.

C. Comparison Analysis of Cause and Prevention Variables-Sample I and Sample II

Were the samples enough alike to combine them for further analysis? If not, how were they different?

To better understand the relationship and differences between the Academic and Corporate/NFP responses, we tested the association of samples (Academic and Corporate/NFP) with each individual prevention and cause item. Adjusted p-values were calculated for the chi-square test statistics, accounting for the clustering of incidents by sampled institutions.³ Rao-Scott design-adjusted p-values were calculated. When the sample size in each of the two groups is 100, which was true for both samples of the CIFAC study, a 0.050 level Chi-square test will have 97% power to distinguish between the groups when the proportions in the 4 categories are characterized by an effect size of 0.1000. Cohen (1988) identifies an effect size of 0.1 as “small.” Therefore, having at least 100 incidents in each sample yields 97% power to detect even small effect sizes.⁴

Regardless of the differences in sample sizes between Academic (315 incidents) and Corporate/NFP (110 incidents), using the adjusted p-values for the chi-square test statistics, we were able to examine the similarity between the two samples. If we discovered that there were no differences between the samples, the entire data set of 430 incidents could be analyzed together. However, if there were statistically significant differences between responses, then those differences would need to be understood and could, in themselves, shed important light on the cause and prevention of incidents.

The Chi square results showed that the samples were remarkably similar. They were significantly different for only 19 of the 81 variables that were compared. Due to differences in samples, 14 of variables were dropped from the comparison analysis. These were variables that measured the effect of a group e.g. faculty not present in the Corporate/NFP environment. Respondents in both samples rated the importance of prevention and cause variables very similarly for most of the study questions. However, they did not rate the variables exactly alike. Therefore, researchers attempted to identify why these 19 variables showed significant differences between the samples.

What were the significant differences? The nineteen different responses are discussed below with plausible explanations given for the differences. We have included one of the tables within the text following item #1 as an example of the values found. (The full set of tables appears in Appendix C of this report.)

1. Increased personnel resources for prevention (p=0.0043);
Academic respondents were more likely to say that this item was quite or extremely important.
Plausible explanation: Within academic institutions, the size of the user population and the IT organizations often require more personnel resources than they have available due to budget restraints.

Ratings for Increased Personnel Resources

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	54	41	13	2	110
% within Sample	49.09%	37.27%	11.82%	1.82%	100.00%
Acad	119	96	60	40	315
% within Sample	37.78%	30.48%	19.05%	12.70%	100.00%
Combined	173	137	73	42	425
% within Sample	40.71%	32.24%	17.18%	9.88%	100.00%

2. Increased audit procedures for prevention (p=0.0114);

³ Rao, J, N, K, & Scott, A. J. (1984) On chi-squared tests for multi-way tables with cell proportions estimated from survey data. *Annals of Statistics*, 12, 46-60.

⁴ Cohen, J (1988). *Statistical Power Analysis for the Behavioral Sciences*, Lawrence Erlbaum Associates, Hillsdale, New Jersey.

Academic respondents were more likely to say that this item was not at all important for prevention.
Plausible explanation: Within educational institutions, the audit functions are more likely to be associated with financial operations than with IT processes and policies. This is again a function of the size and distributed nature of the academic operations and a more traditional way of viewing auditing.

3. Existence of backup for prevention (p=0.0026);

Academic respondents were more likely to say that this item was “not at all” important and less likely to say “somewhat or quite important” than Corporate/NFP respondents.

Plausible explanation: As noted earlier, many of the respondents may have understood the backup function as primarily one for recovery rather than for prevention, and therefore rated this “not at all important” for prevention; this would then be more of a semantic difference than a sample difference.

4. Existence of logging for prevention (p=0.0122)

Academic respondents were more likely to say “not at all” and less likely to say “somewhat important” for preventing incidents than were Corporate/NFP respondents.

Plausible explanation: We are unable to explain this difference. It has been noted during this research however, that many academic institutions, because of a lack of resources, do not actively use logging to detect network malfunctions, attempted access, or other systems problems.

5. Existence of analysis of logs (p=0.0179)

Academic respondents were more likely to say “not at all important” for prevention and less likely to say “somewhat important” than were Corporate/NFP respondents.

Plausible explanation: Like the above explanation this difference could be explained, as a matter of resources, people as well as technical solutions. In some cases, we heard that logging was being done, but that there were no people available to analyze and monitor the logs.

6. Increased requirements for use of personal information for prevention (p=0.0013)

Academic respondents were more likely to say that this variable was “extremely” important for prevention than Corporate/NFP respondents.

Plausible explanation: Given the nature of the Corporate and NFP organizations and their more hierarchical organizational structures, rules and policies may exist regarding where personal information can be stored within the organization and who can have access to such information. These rules are probably not as well established in the more distributed academic environments, thus the need for increased policy to prevent incidents.

7. Increased configuration requirements for mainframe and server software for prevention (p=0.0003)

Academic respondents were more likely to say “not at all important” whereas Corporate and NFP respondents were more likely to say “somewhat, quite, or extremely important.”

Plausible explanation: No explanation is obvious for this response. The Corporate and NFP organizations may, because of their organizational structures, be more capable of asserting requirements over servers and mainframes than the academic environments, where any student or faculty member can purchase and install a server level machine. Implementing configuration requirements in the academic environment is more difficult and therefore may not have been felt plausible to academic respondents.

8. Increased configuration requirements for networks to prevent incidents (p=0.0255)

Academic respondents were more likely to say “not at all important” whereas the Corporate and NFP respondents were more likely to say “somewhat, quite, or extremely important.”

Plausible explanation: One would think that the academic environments, if the above explanation for mainframes and servers is true, would consider it more plausible to place requirements at the network level. There seems to be no obvious explanation for this response.

9. Increased configuration requirements for desktop software to prevent incidents (p=0.0468)

Academic respondents were more likely to say “quite or extremely important” for preventing incidents than Corporate/NFP respondents.

Plausible explanation: Within the academic environments, the desktop software used and its configurations are dependent on the users—students, faculty, and staff. Academic computing environments are heterogeneous environments, whereas in the Corporate and NFP environments, the configurations of desktop software are more often controlled and pushed out for a central load set, by IT personnel. Therefore inserting more controls at the desktop level could be understood as an important preventative measure within the Academic sample.

10. Lack of auditing procedures was seen as important cause of incidents ($p=0.0019$)
The Academic respondents were more likely to say “not at all” and less likely to say “somewhat important” than sample II respondents.

Plausible explanation: Same as #2 above. Academic communities tend to associate the auditing function with financial operations, whereas the sample II respondents tended to see audits as instrumental to full scale checks on policies and procedures, including IT processes.

11. Lack of requirements for the use of personal information as a cause ($p=0.0195$).
Corporate respondents were more likely to say “not at all important” and Academic more likely to say “extremely important.”

Plausible explanation: Same as #6 above.

12. Lack of configuration requirements of mainframe and server software as a cause ($p=0.0373$)
Academic respondents were more likely to say “not at all” and less likely to say “somewhat important” as a cause of incidents.

Plausible explanation: No explanation is obvious for this response. See #7 above.

13. Lack of configuration requirements for desktop hardware as a cause of incidents ($p=0.0072$)
Corporate respondents were more likely to say “not at all” and less likely to say “somewhat important” than were Academic respondents

Plausible explanation: Similar to #9 above. In the academic environments, the selection and configuration of hardware and software for the desktop is often left in the control of the user—the student, faculty member, or staff member. In Corporate environments, there tends to be more standardization of desktop hardware and software, and more central management of those resources.

14. Lack of analysis of logs as a cause of incidents ($p=0.0219$)
Academic respondents were more likely to say that this variable was “extremely important” as a cause of incidents and less likely to say “somewhat important” than were Corporate/NFP respondents.

Plausible explanation: Consistent with the explanation in #5 above, it is plausible that the academic respondents see this lack of process as an important contributor to incidents in their environments. They also may feel that the lack of personnel and lack of automated tools for analyzing logs contribute to the cause of incidents.

15. The number of people affected in an incident as a stimulus to action ($p=0.0496$)
Corporate respondents were more likely to say that the number of people affected was “somewhat or quite important” in causing them to act than were Academic respondents.

Plausible explanation: It is possible that the number of people affected by an incident related directly to productivity and the potential loss of productivity for Corporate and NFP respondents. This ties to the bottom line-operation of their organization and is perhaps taken more seriously as an important factor than it is for academic environments.

16. Number of users the IT system supports ($p < 0.001$)
Academic respondents were more likely to have larger values and Corporate/NFP respondents were more likely to have smaller values.

Plausible explanation: The academic community views their users as faculty, staff and students; in other words both their customers and internal users. Corporate/NFP view their users primarily as their internal staff, with customers not having the need to access the IT equipment.

17. To what extent the IT systems are managed from a central office. ($p < 0.001$)

Corporate/NFP sample was more likely to say quite/extremely, indicating that their systems are more likely to be managed by a centralized office. Academic is more likely to say not at all/somewhat; indicating that their systems are not centralized and managed locally by departments/schools.

Plausible Explanation: The academic community is characterized by having IT resources managed by a IT unit within departments and colleges. By comparison, many corporations/nfps manage and control their IT resources from a central IT department that provides services for the rest of the company.

18. The existence of norms that require IT personnel to involve attorneys in handling incidents. ($p = .0001$)

Academic is more likely to say yes.

Plausible Explanation: Most large colleges and universities have attorneys on staff, so the marginal cost of including an attorney in an incident is low. Participants in the Corporate/NFP sample would incur the cost of an hourly billing rate from a law firm, so it would be costly to involve attorneys.

19. The existence of norms that require IT personnel to involve law enforcement in handling incidents. ($p = .020$)

Academic is more likely to say yes.

Plausible Explanation: Most large colleges have an internal law enforcement/public safety.

V. Cause & Prevention Factors and Best Practices

The size of the CIFAC study and data set allowed researchers to ask deeper questions about the relationship of variables to each other and about their influence on the variance across responses to the study questions. Such analysis has the potential to shed valuable light on the cause of computer-related incidents and on what measures should be taken to prevent incidents from happening. This level of analysis is of particular importance for practitioners within academia and within the Corporate/NFP environments the CIFAC study surveyed. Are there factors to which practitioners, managers and executives should pay particular attention to eliminate some of the computer-related incidents that are occurring? Section A discusses the factors that were identified in each sample. Section B provides a discussion regarding the statistically strongest factors. Section C provides analysis of the recommended best practices.

A. Factors Identified in Each Sample

Do respondents see groupings/clusters of items when they identify Cause or Prevention?

Researchers next asked if there were variables within the cause and prevention questions that clustered together when the participants responded to the items. Were certain variables seen by our respondents as similar in relationship as they responded to the cause questions or to the prevention questions? If certain clusters of variables/factors exist, then it is possible that by addressing those factors one might reduce the number of incidents perceived to be caused by that factor, or be able to prevent certain incidents from happening.

To determine this, statistical data reduction methods, e.g. factor analysis, were used. Cronbach's alpha was used to determine the reliability (average inter-item correlation) of the items loading onto each factor. Items with $\alpha \geq 0.7$ indicated high reliability. Six factors were identified as strongly relating to the cause of computer-related incidents. Eight factors were identified strongly relating to the prevention of computer-related incidents.

Readers are reminded that each of the 134 CIFAC study participants was asked questions regarding 81 different variables for EACH of the 410 incidents that they reported. All of those responses were analyzed. Out of those, six cause variable clusters/factors and eight prevention variable clusters/factors became significant. **Six factors account for over half of the variance in the cause variables from our participant responses within the Academic and the Corporate/NFP samples of the CIFAC study. Eight factors account for greater than half of the variance in the prevention variables from our participant responses within the Academic and the Corporate/NFP samples of the CIFAC study.**

Researchers looked at the variables that were clustering together and assigned them a name that generally reflected the cluster. For example, seven variables clustered together in one of the cause factors. Those variables were:

- Lack or deficiency: Training/Education for IT managers
- Lack or deficiency: Training/Education for IT staff
- Lack or deficiency: Procedures for audit
- Lack or deficiency: Requirements for IT managers
- Lack or deficiency: Requirements for IT staff
- Accidental behavior of IT managers
- Accidental behavior of IT staff

Because these variables clustered together for our respondents as they identified the cause of incidents, we called this cluster "Factor I- Training/Education & Requirements-IT managers/staff." (Appendix D contains the listing of each of the variable clusters for the six cause factors for the Corporate/NFP and Academic samples, and the eight prevention factors for the Corporate/NFP and the Academic samples.) It is important to remember the full set of variables in each cluster as we contemplate each of the factors, by their factor name. By remembering or referring back to the full set of variables in each of the factors, the fuller meaning of the factor can be best understood. In some cases, the exact same factors appeared in both samples, they are noted by an

(*). e.g. The variables in the Training/Education & Requirements: IT Managers/Staff are the same. Even if the factors were not exactly the same, in the variable clusters they represent. e.g. The Academic sample had a cluster of variables involving Management Procedures: Incident response and the Corporate/NFP sample had a cluster titled Management Procedures: Response & Recovery. The only difference for these two clusters is the addition of additional variables indicating the need for management procedures for recovery on behalf of the Corporate/NFP sample. This indicates a high level of similarity between the two samples.

1. Academic Cause Factors

The names that were assigned for the six cause factors in the Academic Sample were Lack or Deficiency in:

- *Factor 1- Training/Education & Requirements: IT Managers/Staff;
- *Factor 2- Training/Education & Requirements: Non-IT Staff;
- Factor 3- Resources & Configuration Requirements: Hardware, Software, Networks;
- Factor 4- Management Procedures: Incident Response;
- Factor 5- Management Procedures: Detecting & Responding-External Users;
- Factor 6- Management Procedures: Recovery;

These factors accounted for 57.3% of the variation in the 38 cause questions for the Academic sample.

2. Corporate/NFP Cause Factors

The names that were assigned for the six cause factors in the Corporate/NFP Sample were Lack or Deficiency in:

- *Factor 1- Training/Education & Requirements: IT Managers /Staff;
- Factor 2- Management Procedures: Detection;
- Factor 3- Management Procedures: Response & Recovery;
- *Factor 4- Training/Education & Requirements: Non-IT Staff;
- Factor 5- Training/Education: External Users;
- Factor 6- Resources & Configuration Requirements-Software and Networks;

These factors accounted for 54.6% of the variation in the 38 cause questions for the Corporate/NFP sample.

3. Academic Prevention Factors

The names that were assigned to the eight prevention factors in the Academic Sample were Increasing or Improvement of:

- Factor 1- Management Procedures: Detection & Response;
- *Factor 2- Training/Education: External Users and Non IT-Staff;
- *Factor 3- Management Procedures: Software;
- *Factor 4- Training/Education & Requirements: IT Staff;
- Factor 5- Management Procedures: Recovery;
- Factor 6- Configuration Requirements: Networks & Desktops;
- Factor 7- Resources: Hardware, Software, Personnel;
- Factor 8- Access Control Requirements: Policy;

These factors accounted for 66.6% of the variance in the 34 prevention questions for the Academic sample.

4. Corporate/NFP Prevention Factors

The names that were assigned to the eight prevention Factors in the Corporate/NFP Sample were Increasing or Improving:

- *Factor 1-Training/Education & Requirements: IT Managers/Staff;
- Factor 2- Management Procedures: Detection, Response & Recovery;
- *Factor 3- Training/Education: External Users & Non IT Staff;
- *Factor 4- Management Procedures: Software;
- Factor 5- Management Procedures: Detection Logging;
- Factor 6- Resources: Hardware, Software, Networks;
- Factor 7- Access Control Requirements;
- Factor 8- Management Procedures: Networks;

These factors accounted for 66.5% of the variance in the 34 prevention questions for the Corporate/NFP sample.

In summary, researchers saw that the cause of a high percentage of incidents had to do with a lack or deficiency of training/education and requirements for IT managers and staff within both sample populations. Our respondents, you will recall, were identified as the people “knowing the most about, or those who handled the computer incidents in their organizations.” They felt that more education and training, as well as more requirements for how work was done, was important in preventing incidents from happening—the lack of such was perceived to be a strong factor in causing computer-related incidents.

Researchers also saw that the cause of a high percentage of incidents had to do with a lack of deficiency of education and requirements for Non-IT staff within both sample populations. Likewise, the prevention of such incidents could be accomplished, in the opinion of our respondents, by provision of such training/education and requirements.

In both samples, researchers saw the importance of lack of or deficiency of management procedures for incident detection, response, and recovery as a cause of incidents. For preventing incidents, our respondents identified increasing and improving such management procedures as important.

The Academic and Corporate/NFP samples differed slightly in other factors which each sample found important. Like the analysis which was done in Volume I of the CIFAC study, however, the factors that were identified primarily focused on the people—their training, education, and performance requirements, not on inadequacies or lack of technologies or technical functionality. In Volume I researchers wrote:

“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.”⁵

These quotes from Volume I can be echoed in this second volume. The CIFAC study has highlighted and confirmed that computer incidents require attention to people, process and technology. Executive leadership of Colleges, Universities, Corporations and Not-for profit organizations must focus on people and processes to improve security and protect against systems, data and people-focused computer incidents. Looking at security as if it were a technology issue will not address the cause of computer incidents. A member of the CIFAC advisory board, Jack Suess put it succinctly when he said:

“...organizations must focus on the harder and more complex challenges of changing behavior through training, developing processes and procedures, and following up [to ensure] that training is happening and that the processes and procedures are being followed.”

⁵ Rezmierski, V., Rothschild, D., Kazanis, A., & Rivas, R. 2005. Final Report of the Computer Incident Factor Analysis and Categorization (CIFAC) Project: Volume I: College and University Sample. The University of Michigan.

B. Analysis of Variance

Can we identify the Cause of, or how to Prevent, certain types of incidents?

Knowing that 6 factors account for nearly half of the variance of responses to cause questions and 8 factors account for over half of the variance of responses to prevention questions is important. However, it is important to ask, do these factors tell us anything about the cause of, or how to prevent, specific types of incidents—data, systems, or people—as categorized in the CIFAC study? E.g., Can we prevent “data” incidents from happening by doing the things called for in Factor X? Do these factors tell us anything about the cause of, or how to PREVENT the most serious of the incidents reported by our respondents? E.g. Can we prevent the “extremely serious” incidents from happening by doing the things called for in Factor Y?

To answer these questions, researchers performed analysis of variance for categories of incident type and for the range of incident seriousness.

If the variables clustered in each of the 6 factors for cause and the 8 factors for prevention, were the same in the Academic and in the Corporate/NFP sample, then researchers could combine the responses and analyze the factors as one total sample. Based on statistical analysis, however, it was determined that the two samples were not sufficiently similar to combine the samples for this factor analysis. Therefore, factors related to cause and those related to prevention will be discussed separately for the Academic and for the Corporate/NFP samples for analysis of incident types (data, systems, people), and for incident seriousness (not at all, somewhat, quite, and extremely.) Our respondents in the two samples saw things differently as they identified aspects of cause or prevention for their Academic or Corporate environments.

An analysis of variance (ANOVA) allows researchers to identify those factors that have significantly different means relative to different types of incidents (data, systems, people), that is....the factors that have a greater association with the cause or prevention of particular types of incidents. Likewise, an ANOVA allows researchers to identify those factors that have significantly different means for incidents of different seriousness levels; that is.....the factors that have a greater association with the cause/prevention of incidents at different levels of seriousness.

Researchers asked:

- What factors are perceived as causing different types of incidents (system, data, people)?
- What factors, if addressed, could prevent incidents of different types from happening?
- What factors are perceived as causing the most serious incidents?
- What factors, if addressed, could prevent the most serious incidents from happening?

1. Results of ANOVA for Cause Related to Type of Incident

What factors are related to the Cause of certain types of incidents?

Academic Sample

- a. The strongest cause factors for the systems incidents were Lack or Deficiency in:
Factor 1 – Training/Education & Requirements: IT Managers/Staff;
Factor 5 – Management Procedures: Detecting & Responding – External Users;
- b. A cause factor for data incidents was Lack or Deficiency in:
Factor 2 – Training/Education & Requirements: Non-IT Staff;
- c. No strong cause factors were identified for people incidents.

Corporate and Not-for-Profit Sample

- a. The strongest cause factors for systems incidents were Lack or Deficiency in:
Factor 2 – Management Procedures: Detection;
Factor 5 – Training/Education: External Users;

- b. A cause factor for people incidents was Lack or Deficiency in:
Factor 4 – Training/Education & Requirements: Non-IT Staff;
- c. No strong cause factors were seen in the Corporate sample for data incidents.

As a cause of computer-related incidents, researchers concluded that for both of the CIFAC study samples, lack or deficiency of training/education played an important role in causing computer incidents.

2. Results of ANOVA for cause related to Seriousness of incident
What factors are seen as the cause of the most serious incidents?

Academic Sample

- a. The strongest cause factors for the “extremely serious” incidents in the Academic sample were Lack or Deficiency in:
Factor 2 – Training/Education & Requirements: Non-IT Staff;
Factor 6 – Management Procedures: Recovery;
- a. A cause fact or for those incidents identified as “quite serious” was Lack or Deficiency in:
Factor 1 – Training/Education & Requirements: IT Managers/Staff;

Corporate Sample

- a. No strong cause factors were seen in the Corporate/NFP sample for incidents of different levels of seriousness.

Training/education and requirements for IT managers and staff and for non IT staff members is an important--perhaps critical-- process to be addressed in order to eliminate the cause of many of the systems, data, and most serious of the incidents that are occurring.

3. Results of ANOVA for Prevention related to type of incident
Are there factors that, if addressed, could prevent certain types of incidents?

Academic Sample

Researchers found, for the Academic sample, the following results relative to prevention:

- a. The strongest prevention factors for systems incidents were Increasing or Improving:
Factor 3 – Management Procedures: Software;
Factor 5 – Management Procedures: Recovery;
Factor 6 – Configuration Requirements Networks & Desktops;
Factor 7 – Resources: Hardware, Software & Personnel;
- b. The strongest prevention factors for people incidents were Increasing or Improving:
Factor 2 – Training/Education: External Users & Non-IT Staff;
Factor 8 – Access Control Requirements: Policy;
- c. No strong prevention factors were seen for data incidents.

Corporate Sample

Researchers found, for the Corporate/NFP sample, the following prevention results:

- a. No prevention factors were identified for systems incidents in the Corporate/NFP sample.
- b. The strongest prevention factors for people incidents were Increasing or Improving:
Factor 3 – Training/Education: External Users & Non-IT Staff;

Factor 7 – Access Control Requirements;

c. A prevention factor for data incidents was Increasing or Improving:
Factor 7 – Access Control Requirements;

To prevent computer-related incidents from happening, researchers found, for both of the CIFAC study samples, that increased management procedures and increased access control requirements would play an important role. Again, increased training/education for non-IT staff and for external users was seen as a necessary measure for preventing computer-related incidents.

4. Results of ANOVA for prevention related to Seriousness of incident
Are there factors that, if addressed, could prevent the most serious incidents from happening?

Academic Sample

a. The strongest prevention factors for the “extremely serious” incidents in the Academic sample were Increasing or Improving:

Factor 5 – Management Procedures: Recovery;

Factor 7 – Resources: Hardware, Software & Personnel;

b. No strong factors were identified for the “quite serious” incidents in the Academic sample.

In the Academic sample, increased hardware, software and personnel resources were also felt to be related to preventing the most serious systems incidents from occurring.

Corporate Sample

a. The strongest prevention factors for extremely serious incidents in the Corporate/NFP sample were Increasing or Improving:

Factor 2: Management Procedures: Detection, Response & Recovery;

Factor 7: Access Control Requirements;

b. A prevention factor for incidents judged to be quite serious was Increasing or Improving:
Factor 8 – Management Procedures: Networks;

Corporate respondents saw increased access control requirements and management procedures for detection, response and recovery as most important in addressing the most serious of the computer-related incidents. Addressing the need for increased management procedures and access control could prevent the extremely serious incidents from occurring.

C. Analysis of Best Practices

Are there particular best practices that were recommended by respondents for different types of incidents, for incidents of different levels of severity, or according to the sample from which they came?

Each CIFAC respondent, in relation to the incident they were describing, was asked to identify best practices to share with colleagues. They were asked to identify a “best practice for preventing the incident,” “a best practice for mitigating the effects of the incident,” and a “best practice for managing the incident.” This input from the respondents was provided in narrative –non-numerical form. To prepare the answers for analysis, a multi-rater scoring methodology was used; three members of the CIFAC research team read each recommended best practice and assigned each a score according to categories defined in Appendix E of this report. E.g., if one of our respondents recommended a best practice for preventing the reported incident using language such as “teach the user this company’s rules for what is and isn’t allowed”, the research team members would likely rate that

response a '2' according to the definitions because it most nearly matched definition 2 "education, training, awareness and straightforward communication".

For prevention best practices the three CIFAC raters classified the narrative response into one of the following categories:

1. Nothing-no preventative measure
2. Education, training, awareness, and straightforward communication
3. Test, patch, debug, and procedures therefore
4. Have and follow procedures, policies, and standards
5. Technical preventative controls
6. Missing data or a response of "don't know".

For mitigation best practices, the raters classified the narrative response into one of the following:

1. Administrative collaboration and communication
2. Education, training, awareness, and straightforward communication
3. Take decisive and timely action
4. Have and follow procedures, policies, and standards
5. Remove or quarantine cause of problem;
6. Missing data or "don't know".

For management best practices, the raters classified the narrative response into one of the following:

1. Administrative collaboration and communication
2. Education, training, awareness, and straightforward communication
3. Take decisive and timely action
4. Have and follow procedures, policies, and standards
5. Log and document incident.

With three independent raters, and considering the individualistic language of 134 participants, however, it was not always clear which definition was the closest to the respondent's intended best practice. To identify a single rating for each item, the most common rating was assigned as the overall rating from the three CIFAC raters. E.g., if the three CIFAC raters assigned '2', '3', '2', respectively, '2' was entered as the most common and therefore the overall rating for that recommended best practice.

For prevention items, since a '1' response was defined as "nothing-no preventative measure" and a '9' as "don't know what could be done to prevent this", these two items were combined for analysis. This was not the case for the mitigation or management recommended best practices where each of the ratings held distinct content and only '9' stood alone representing missing data or a "don't know" response

The overall score was assigned, as described above, with four exceptions which necessitated that best practice to be dropped from the analysis as invalid. The four exceptions were:

- a) If one of the three CIFAC raters entered a score but the other two could not decide a rating e.g. 1, _, _
- b) If one rater could not decide a rating and the other two selected different scores e.g. _, 2, 4
- c) If all three raters entered a score but all three were different. e.g. 2, 4, 5
- d) If none of the three raters could decide an appropriate score for the best practice submitted by the respondent. e.g. _, _, _

Multinomial logistic regression models were fitted to a single data set combining the Academic and Corporate/NFP samples (n=429). By including sample as one of the predictor variables, it allowed researchers to combine all the recommended best practices and analyze the response as a single data set. The dependent variable was the overall recommended best practice (or the most common rating of the three CIFAC raters for each incident.) The predictor variables included focus of incident, seriousness of incident, and sample (Academic or Corporate/NFP).

1. Results from Analysis of Prevention Best Practices

When researchers scored the best practices for prevention, 73.4% of the Academic best practices and 72.7% of the Corporate/NFP returned a valid rating. Based upon these results, it is shown that Education and Training, Test, Patch, and Debugging Procedures, Technical Preventative Controls, and having Policies and Procedures were seen as important best practices for preventing incidents. For the Academic sample (27.6%), and overall (24.0%), Education Training, Awareness and Straightforward Communication were most frequently identified. In the Corporate/NFP sample, Test, Patch, Debug and Procedures therefore was most frequently identified (23.6%) as the best practice for prevention.

Prevention Best Practices

Prevention	Academic		Corp/NFP		Total	
Nothing	10	3.13%	1	0.91%	11	2.56%
Education, training, awareness, and straightforwardness	88	27.59%	15	13.64%	103	24.01%
Test, patch, debug, and procedures therefore	39	12.23%	26	23.64%	65	15.15%
Have and follow procedures, policies, and standards	33	10.34%	22	20.00%	55	12.82%
Technical preventative controls	49	15.36%	16	14.55%	65	15.15%
Exceptions	100	31.35%	30	27.27%	130	30.30%
Total	319	100.00%	110	100.00%	429	100.00%

To determine whether incident focus (people, data, systems,) seriousness (not at all, somewhat, quite, or extremely) or the sample (Academic or Corporate/NFP,) was associated with a particular best practice for prevention, the associations of the predictors with the best practice responses were tested using Wald chi-square tests.. In analyzing the best practice responses, researchers combined '1' ratings which indicated "nothing could be done" with '9' ratings which indicated "missing or don't know" and the combined category '9' was used as a baseline. If a best practice response was significantly different then this combined indicator, some effect of the variable, (focus, seriousness or sample) was being realized. In other words, researchers asked, did incident focus, seriousness, or the sample make any of these recommendations, aside from the baseline, significantly more or less likely? Wald chi-square tests indicated that incident focus, incident seriousness, and sample were all significant predictors of recommended best practice at the 5% level.

Recommended Best Practices for the Prevention of People Incidents

In terms of the **focus** results, **people** incidents were significantly more likely than systems incidents to result in a recommended best practice of '2' relative to a recommended best practice of '9'. That is, those incidents where the focus of the incident was judged to be people were significantly more likely to have an assigned best practice of "Education, training, awareness, and straight-forward communication" given by our respondents. Nearly 51% of people incidents had a recommended best practice of '2.' Only 12.9% of the systems incidents had that best practice given.

Prevention Best Practices by Focus

BP Category	1&9	2	3	4	5	Total
People	7	53	14	16	14	104
% within focus	6.73%	50.96%	13.46%	15.38%	13.46%	100.00%
Data	9	33	10	21	10	83
% within focus	10.84%	39.76%	12.05%	25.30%	12.05%	100.00%
Systems	9	16	40	18	41	124
% within focus	7.26%	12.90%	32.26%	14.52%	33.06%	100.00%
Total	25	102	64	55	65	311
% within focus	8.04%	32.80%	20.58%	17.68%	20.90%	100.00%

Recommended Best Practices for the Prevention of Extremely and Quite Serious Incidents

In terms of the **seriousness** results, incidents rated “**Extremely**” or “**Quite**” were both less likely to have a recommended best practice for prevention of ‘2’ relative to a RBP of ‘9’ –“nothing or don’t know”. Further, incidents rated “not at all” or “somewhat” serious were significantly more likely to have a rating of ‘4’ –“Have and follow procedures, policies, and standards” than a ‘9’.

Prevention Best Practices by Seriousness

BP Category	1&9	2	3	4	5	Total
Not at All/Somewhat	2	39	16	16	16	89
% within seriousness	2.25%	43.82%	17.98%	17.98%	17.98%	100.00%
Quite	11	24	26	11	28	100
% within seriousness	11.00%	24.00%	26.00%	11.00%	28.00%	100.00%
Extremely	13	40	22	28	21	124
% within seriousness	10.48%	32.26%	17.74%	22.58%	16.94%	100.00%
Total	26	103	64	55	65	313
% within seriousness	8.31%	32.91%	20.45%	17.57%	20.77%	100.00%

Recommended Best Practices for Prevention of Incidents by Samples

In terms of the **sample**, incidents for the **Corporate/NFP** sample are significantly more likely to be assigned a recommended best practice for prevention of ‘3’, ‘4’, and ‘5’ than a ‘9’. Best practice ‘3’ is “, patch, debug and procedures therefore”. Best practice ‘4’ is –“have and follow procedures, policies and standards”. Best practice ‘5’ is – “have technical preventative control mechanisms”.

In the **Academic** sample, nearly 11% of the incidents have a recommended best practice of ‘9’ “nothing or don’t know”. Specifically, the relative proportions of ‘3’ to ‘9’, ‘4’ to ‘9’, and ‘5’ to ‘9’ were all significantly larger in the corporate sample.

Prevention Best Practices by Sample

BP Category	1&9	2	3	4	5	Total
Academic	25	88	39	33	49	234
% within	10.68%	37.61%	16.67%	14.10%	20.94%	100.00%
Corporate/NFP	1	15	26	22	16	80
% within	1.25%	18.75%	32.50%	27.50%	20.00%	100.00%
Total	26	103	65	55	65	314
% within	8.28%	32.80%	20.70%	17.52%	20.70%	100.00%

2. Results from Analysis of Mitigation Best Practices

Analysis showed that 67.6% of the ratings for the mitigation best practices produced a valid recommended best practice. With 18.4% of the overall ratings, education and training was viewed to be the most important best practice for mitigation. It was followed by “remove the problem” (12.4%) and “take decisive and timely action.” Again, education, training, awareness and straightforward communication were identified in the Academic sample most frequently identified (19.8%) as the best practice. In the Corporate/NFP sample, having and following policies, procedures and standards was most frequently identified (20.0%) as the best practice.

Mitigation Best Practices

	Academic		Corp/NFP		Total	
Administrative collaboration and communication	20	6.27%	5	4.55%	25	5.83%
Education, training, awareness, and straightforwardness	63	19.75%	16	14.55%	79	18.41%
Take decisive and timely action	38	11.91%	10	9.09%	48	11.19%
Have and follow procedures, policies, and standards	17	5.33%	22	20.00%	39	9.09%
Remove or quarantine cause of problem	41	12.85%	12	10.91%	53	12.35%
Exceptions	140	43.89%	45	40.91%	185	43.12%
Total	319	100.00%	110	100.00%	429	100.00%

Overall, Wald chi-square tests indicated that the level of incident seriousness (not at all, somewhat, quite, or extremely) was not a significant predictor of recommended best practices for mitigation. Incident focus (systems, data, or people) and the sample (Academic or Corporate/NFP) were both significant predictors of recommended best practices at the 5% level.

Recommended Best Practices for the Mitigation by Focus

In terms of the **focus** results, **systems** incidents are significantly more likely than both people and data incidents to result in a recommended best practice of '5' relative to '9' - "nothing or don't know." Respondents recommended '5' - "Removing or quarantining the cause of the problem" for mitigating systems incidents.

Mitigation Best Practices by Focus

BP Category	1	2	3	4	5	9	Total
People	13	33	17	18	8	15	104
% within focus	12.50%	31.73%	16.35%	17.31%	7.69%	14.42%	100.00%
Data	3	23	13	9	5	16	69
% within focus	4.35%	33.33%	18.84%	13.04%	7.25%	23.19%	100.00%
Systems	9	22	18	12	39	14	114
% within focus	7.89%	19.30%	15.79%	10.53%	34.21%	12.28%	100.00%
Total	25	78	48	39	52	45	287
% within focus	8.71%	27.18%	16.72%	13.59%	18.12%	15.68%	100.00%

Recommended Best Practices for the Mitigation of Incidents by Sample

In terms of the **sample** results, the **Corporate/NFP** sample is significantly more likely to have recommended best practices of '2' - "Education, training, awareness, and straightforward communication," '4' - "Have and follow procedures, policies, and standards," and '5' - "Remove or quarantine cause of problem," relative to a RBP of '9' - "nothing or don't know." **Academic** respondents were more likely to have said "nothing or don't know" in response to mitigating effects.

Mitigation Best Practices by Sample

BP Category	1	2	3	4	5	9	Total
Academic	20	63	38	17	41	43	222
% within sample	9.01%	28.38%	17.12%	7.66%	18.47%	19.37%	100.00%
Corporate/NFP	5	16	10	22	12	3	68
% within sample	7.35%	23.53%	14.71%	32.35%	17.65%	4.41%	100.00%
Total	25	79	48	39	53	46	290
% within focus	8.62%	27.24%	16.55%	13.45%	18.28%	15.86%	100.00%

3. Results from Analysis of Management Best Practices

With 75.29% of the ratings being valid, administrative collaboration was recommended 22.8% of the time, almost 10% more than the next closest recommended best practice of having policies and procedures (13.3%). Education was once again emphasized for management and was recommended at 11.7% of the time. In both the Academic and Corporate/NFP samples, “Administrative collaboration and communication” was the most frequently recommended best practice (23.5% and 20.9%, respectively).

Management Best Practices

Management	Academic		Corp/NFP		Total	
Administrative collaboration and communication	75	23.51%	23	20.91%	98	22.84%
Education, training, awareness, and straightforwardness	38	11.91%	12	10.91%	50	11.66%
Take decisive and timely action	30	9.40%	9	8.18%	39	9.09%
Have and follow procedures, policies, and standards	36	11.29%	21	19.09%	57	13.29%
Log and document incident	26	8.15%	10	9.09%	36	8.39%
Exceptions	114	35.74%	35	31.82%	149	34.73%
Total	319	100.00%	110	100.00%	429	100.00%

Wald chi-square tests indicated that seriousness and incident focus were not significant predictors of the recommended best practices for management of incidents. Sample was a significant predictor of recommended best practice at the 5% level.

Recommended Best Practice for Management by Sample

The **Corporate** sample was significantly more likely to have a recommended best practice of ‘1’- “administrative collaboration and communication”, ‘2’-“Education, training, awareness, and straight forward communication”, ‘3’- “take decisive and timely action”, ‘4’ –“Have and follow procedures, policies, and standards”, or ‘5’ –“Log and document the incident” for management, relative to a recommended best practice of ‘9’-“nothing or don’t know.” They were much more likely to say ‘1’ or ‘3’. The Academic sample was much more likely to say ‘9’ –“nothing or don’t know” in response to best practice for managing incidents.

Management Best Practices by Sample

BP Category	1	2	3	4	5	9	Total
Academic	75	38	30	36	26	42	247
% within sample	30.36%	15.38%	12.15%	14.57%	10.53%	17.00%	100.00%
Corporate/NFP	23	12	9	21	10	1	76
% within sample	30.26%	15.79%	11.84%	27.63%	13.16%	1.32%	100.00%
Total	98	50	39	57	36	43	323
%	30.34%	15.48%	12.07%	17.65%	11.15%	13.31%	100.00%

Summary of Best Practice Analysis

In summary, when analyzed against the possibility of saying “don’t know” as a response to recommending a best practice, incident type, seriousness, and/or the sample had statistically significance influences on some of the of the best practices that were selected by our respondents

For **preventing incidents, type, seriousness, and sample** influenced the recommendation of best practice. For people incidents, our respondents recommended education, training, awareness training, and straight-forward communications. To prevent the **most serious** incidents, our respondents recommended having and following procedures, policies and standards. Within the Corporate/NFP sample, respondents recommended testing,

patching, debugging procedures, having and following procedures, policies, and standards, and technical preventative controls as best practices. No best practice was more likely than a response of “nothing or don’t know” for data type incidents.

For **mitigating** the effects of incidents, only **focus** and **sample** influenced recommended best practices. For the mitigation of systems incidents, our respondents recommended having and following procedures, policies, and standards. The Corporate/NFP sample recommended having and following procedures, policies, and standards for mitigating the effects of incidents.

For **managing** incidents, only **sample** influenced recommended best practices. Type and seriousness were not significant in influencing best practices. The Corporate/NFP sample recommended administrative collaboration and communication as well as having and following procedures, policies, and standards as best practices.

VI. CONCLUSIONS, RECOMMENDATIONS AND REFLECTIONS

In this section of the Final Report-Volume II-Corporate and NFP Sample, the researchers will summarize key findings and make recommendations that we believe come directly from the study results.

The Computer Incident Factor Analysis and Categorization project, CIFAC, used a people-intense methodology of in-person interviews to collect descriptions of, and extensive data about, 430 computer-related incidents. Incidents were collected from 134 participants in 36 colleges and universities and 28 corporations and NFP organizations. Using a broad definition of computer-related incident to capture data on a wide range of incidents within these organizations, the CIFAC study examined the use of a three part categorization model for characterizing incidents based on the incident focus—people, systems or data. Researchers collected data on 81 variables for each of the 430 incidents and also solicited recommended best practices for preventing each of the incidents, for mitigating the effects of the incident, and for managing the incident.

A. Conclusions

1. Size and Centralization Differences in Samples

The first study to examine explicit data from real incidents in both Academic and Corporate/NFP samples, the CIFAC study found that responses to cause and prevention questions were very similar across the two samples. There was no significant difference in the way respondents assigned importance to 64 of the 81 cause and prevention variables. Only 19 of the variables in the entire study showed significant differences between the two samples. The differences appeared to be a function of the different organizational structures, the centralization of IT services and the size and definition of “user population” in each of the settings.

The Corporate/NFP organizations seemed better equipped with policies and requirements already in place and sought more detection and response mechanisms to prevent incidents. The Academic environments appeared to need more policies, procedures, and requirements. Corporate/NFP settings also engaged auditors in routinely monitoring their management procedures, including information technology operations. Academic institutions, on the other hand, appeared to primarily involve auditors for financial operations rather than IT practices and procedures. Users were defined differently in these two settings as well. The IT user population for Academic institutions is much larger as it includes faculty and students. The Corporate user population appears to be generally restricted to individuals over whom the organization has contractual control—employees and external contractors.

The explanations of organizational structure and centralization and size which were given by the researchers explaining the differences between these two samples in the way they responded to 19 of the study variables was reinforced by the data as well. Demographic data collected during the study showed that there was a significant difference between these two samples in number of users. For the Corporate/NFP sample, 21% had user populations less than 500 and 21% had user populations greater than 5,000 but less than 20,000. For the Academic sample, 30% of the colleges/universities had user populations greater than 5,000 but less than 20,000 and 42% had user populations greater than 20,000 but less than 50,000. With these number differences in size, it is no surprise that Academic respondents were more likely than Corporate/NFP to identify the need for more personnel resources and for more policies and procedures to prevent computer-related incidents.

Demographic data collected during the study also showed that there was a significant difference between these two samples in the degree to which their IT service organizations were centralized. Forty-five percent of Corporate respondents, in response to the question “how centralized are your IT services” said that their services were extremely centralized. Only 24% of Academic respondents indicated “extremely” centralized. Nearly 80% of Corporate respondents indicated that their IT services were “quite or extremely” centralized as opposed to 56% of Academic respondents. 41% of Academic respondents said that their services were only “somewhat” centralized as opposed to 21% of Corporate respondents.

Given this fact of more centralization of services within Corporate/NFP organizations, it is also not surprising that the Corporate organizations did not feel the same urgency for greater configuration requirements for desktop computers. They have the ability to set the configuration requirements and enforce them within departments whereas in the Academic environments, individual departments and even individual faculty or students may control what configurations are in place on individual machines.

2. Factors Related to Cause and Prevention of Incidents

The CIFAC study researchers found 6 factors which are statistically related to the cause of incidents in the Academic and in the Corporate/NFP samples and 8 factors that are statistically related to the prevention of computer incidents in each of the samples. These factors account for over half of the variance in participant responses within the samples. These factors, which represent clusters of variables associated with cause or with prevention of incidents, do not represent opinions. Rather, they are statistically derived from the analysis of hundreds of participant answers to the importance of 81 variables within the study questions.

The data show that the cause of a high percentage of incidents had to do with a lack or deficiency of education and requirements for IT managers and staff within both sample populations. The data show that the cause of a high percentage of incidents had to do with a lack or deficiency of training/education and requirements for non-IT staff within both population samples as well. These factors—training/education and requirements for IT managers and staff, and education and requirements for non-IT staff, showed up repeatedly throughout this study. They are significant cause factors for the incidents, and are seen, if addressed, as significant for preventing incidents from happening in the future.

The data also show that the cause factor for a high percentage of incidents had to do with a lack or deficiency of management procedures for incident detection, response, and recovery. Having more and better management procedures in place at the start of an incident was seen as important in preventing that, and future, incident(s) from happening.

The Academic and Corporate/NFP samples differed slightly in other factors which each sample found important. Like the analysis which was done in Volume I of the CIFAC study, however, the factors that were identified primarily focused on people—their training, education, and performance requirements, not on inadequacies or lack of technologies or technical functionality.

3. Factors Related to Specific Types of Incidents and to Specific Levels of Incident Seriousness

In addition to identifying the factors related to cause and prevention, researchers analyzed the relationship between types of incidents—data, systems, or people, and the identified factors and between incident seriousness and the factors. Their analysis repeatedly identified increased and more adequate education and training for IT managers, IT staff, and non-IT staff as important for preventing people, systems and data incidents. The factors were related to the cause of extremely serious incidents as well, pointing out the need for more and better management procedures.

To specifically highlight some of the types of education and procedures that are needed, researchers have provided recommendations for policies, procedures, and education.

4. Conclusions Relative to Best Practices

For best practices, when analyzed against the possibility of saying “don’t know” as a response to recommending a best practice, incident type, seriousness, and/or the sample, had statistically significant influence on some of the best practices that were selected by our respondents.

For preventing incidents, type, seriousness, and sample influenced the recommendation of best practice. For people incidents, our respondents recommended education, training, awareness training, and straight-forward communications. To prevent the most serious incidents, our respondents recommended having and following

procedures, policies and standards. Within the Corporate/NFP sample, respondents recommended testing, patching, debugging procedures, having and following procedures, policies, and standards, and technical preventative controls as best practices. No best practice was more likely than a response of “nothing or don’t know” for data type incidents.

For mitigating the effects of incidents, only focus and sample influenced recommended best practices. For the mitigation of systems incidents, our respondents recommended having and following procedures, policies, and standards. The Corporate/NFP sample recommended having and following procedures, policies, and standards for mitigating the effects of incidents.

For managing incidents, only sample influenced recommended best practices. Type and seriousness were not significant in influencing best practices. The Corporate/NFP sample recommended administrative collaboration and communication as well as having and following procedures, policies, and standards as best practices.

B. RECOMMENDATIONS:

On the basis of this research and our experience during the CIFAC study, we recommend:

1. Continuation of the trend that we observed during this data collection, to increase the centralization of key IT services, especially security processes and procedures, and the distribution of policies.
2. The creation of stronger and more explicit procedures and requirements for IT staff performance.
3. The establishment of explicit organizational requirements for desktop configurations which can be enforced through the networks.
4. That Academic IT managers engage auditors to help them monitor the implementation of policies and compliance with set requirements and procedures for the management of IT resources.
5. That Corporate/NFP IT managers more actively employ logging, analysis of logs, and other detection and response procedures for identifying potential incidents, especially in relation to external contractor/users.

1. Relative to Policy

We recommend that the both Academic and Corporate/NFP organizations establish policies (if they are not already in place) for the following:

- Disposal of hardware and software
- Proper use of systems for external users and contractors
- Identification of and proper use of copyrighted works
- Use and protection of multiuse passwords
- Organizational limits on bandwidth use
- What, where, and how to backup and how it should be done, managed, and stored
- Configuration requirements for networks
- Configuration requirements for desktop machines
- Data classification and appropriate sensitivity level protections
- Hardware and software update schedules
- Software vulnerability assessment, management, and patching

2. Relative to Operational Procedures

We recommend that both Academic and Corporate/NFP organizations establish specific procedural check lists and administrative procedures for:

- Configuration testing
- Backup, testing, and disaster recovery
- Network and system vulnerability testing and patching

- Routine auditing of procedures and policies
- Routine (physical and virtual) risk management assessment and reporting
- Protection of root access on major servers; restriction of the number of people with such access and rapid termination of such access privileges upon job changes
- Consistency and quality checking on routine procedures e.g. checklists and cross checks for procedures that are done by multiple persons or are done routinely and are subject to error
- Testing and patching all new installations
- Full testing prior to implementations of all new or updated systems
- Clarification of job requirements for all IT personnel- aligned to skill levels
- Requirements for the use of test environments for unstable systems rather than testing systems in production environments
- Required periodic password changing or at a minimum, bi-annual system-wide vulnerability identification and notification for users of multiuse passwords

3. Relative to Education and Training for IT Managers

We recommend that both Academic and Corporate/NFP organizations provide the following education and training for IT managers (if such is not already available within the organizations):

- How to create specific performance checklists to ensure consistent performance of routine and repeated actions by IT staff
- On-going technical training to ensure progressive knowledge regarding different operating systems and their interactions within rapidly changing networked environments
- How to identify and specify the specific job skill sets required for the performance of specific operations by their IT staff
- How to monitor and oversee staff progress to higher levels of performance and compensation
- How to identify of and implement redundant systems where critical services exist
- How to identify and engage the routine oversight processes to ensure implementation of policies and standards and the reduction of enterprise risks e.g. involving risk managers, auditors, and supervision for oversight and review
- How to identify and establish interdisciplinary teams for the handling, when needed, of computer-related incidents
- On-going education regarding legal, organizational policy, and human resource issues and requirements
- Training in efficient, effective, and collaborative communication with key administrators and with the general user population when incidents occur and how they are being managed

4. Relative to Education and Training for IT AND non-IT Staff

We recommend that both Academic and Corporate/NFP organizations provide the following educational programs for IT staff (if they are not already available and routinely implemented within the organizations):

- Data sensitivity levels and data protection procedures commensurate with sensitivity levels
- Locking workstations using Windows key L when not in use
- How to follow procedural checklists without shortcuts
- Adequate and appropriate documentation of systems when changes are made
- Password protections and routine changing
- Responsibility for their personal workstation and for data stored there
- On-going basic security awareness and consistent implementation of basic computer security measures and checks
- Understanding the limits of their job description and data management responsibilities and where their authorizations stop
- On-going training regarding organizational policies and requirements in the use of information and technology resources
- Periodic education regarding configuration requirements for their desktop machines
- Awareness of the IT management's responsibility and obligation to investigate and monitor behaviors on the network that have the potential to disrupt services
- Thorough and routine education regarding organizational policies, relevant laws, and human resource requirements in the use of information and IT resources

C. Reflections

1. Role of Centralization

Though it was not a surprise to researchers, a significant difference existed in how centralized IT services are, between the two samples. Corporate/NFP are more likely to have centralized IT functions within their organization. With the advent of personal computers, corporations and academia both moved from centralized mainframes to computing on the desktop. Within academia, a decentralization of IT services to departments and Academic units followed. As the data shows, the Corporations and NFPs continued to keep their IT services centralized within their organizations. Even though there are incidents occurring in both the centralized and de-centralized environments, there are items that can be learned from each sample.

Due to many factors, it would be difficult to place the proverbial genie back in the bottle and centralize IT services academia. However, there are things that the Academic community could do to help reduce the number of incidents that occur on their campuses. For instance, enforcing policies which govern the use of the network is one such way. One such area of policy that could be created, enforced and audited is the ability of a computer to join the network. By requiring such things as port scans, the need to have a fully-patched machine and up-to-date virus software, before a device can join the network, colleges and universities can reduce the number of incidents by quarantining a problem before it created havoc. Such a policy could be politically difficult to implement and enforce. An audience member at a conference mentioned that in corporations IT departments have the right of refusal and are involved in the planning phase for projects from the beginning. However, due to Academic freedom or a researcher receiving a grant, IT departments in colleges/universities do not always have the right of refusal or the ability to properly plan for a new server to join the network. In order to reduce exposure and the likelihood of incidents occurring, centralized policy making is important in the college/university environment.

Other items academia could implement that are regularly used in the Corporate world include:

- Use of test environments to reduce the release of buggy software
- Use of a standard load set that includes patches for desktop machines
- Increased requirements for the use of personal information

2. Categorization System

For the CIFAC study, researchers created and asked respondents to categorize incidents based upon their focus, whether it is data, people or systems. In volume 1 of the CIFAC report, researchers noted:

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.

At the conclusion of the Corporate/NFP sample, researchers continue to find the above scenario to be true. As in the Academic sample, respondents in the Corporate/NFP sample had difficulty in the use of this system of describing incidents. As in volume I, we find ourselves asking the following question:

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

This categorization system continues to be difficult to be interpret. However, researchers believe that with a slight modification this categorization could be more useful. Many respondents attempted to discern what ‘focus’ meant. Some interpreted it as the intended target of a perpetrator’s actions. E.g. If the actor was trying to harm an individual, the respondent interpreted it as a ‘people’ incident. Others interpreted focus to mean what action they should take in the handling of the incident. If they had to secure the data, they called it a ‘data’ incident. Therefore, by defining what the ‘focus’ of the incident means, this system could evolve and become more useful. More clarity, especially in the definition of ‘focus’ will be needed before practitioners can use this system for categorizing incidents. The fact that there is a significant association between type of incident & best practice means that this categorization system could help practitioners get to interventions and “best practices” quicker if incident type were correctly categorized.

3. Incidents Can and Will Happen

Researchers realize that there is only so much you can do to prevent incidents. This is apparent in our research when incidents occur where there appears to be no way to prevent an incident from happening. Examples from our research include the following:

- Individuals who have a strong intention of doing harm
- The existence of unknown vulnerabilities/bugs in software
- Previously unknown viruses, spyware and other malicious software
- Hackers and script kiddies exploiting vulnerabilities
- Emotionally disturbed, immature and/or irrational users.

However there are things that can be done to reduce risk of these incidents happening and the impact that it will have on an organization. Some examples of how to reduce these incidents are discussed throughout the report and include ensuring that you have policies and procedures in place to update computers as patches come out, plans and procedures in place for when an unknown bug in software is in place, the use of access control tools to limit access to sensitive areas and data and properly educating IT staff in the use of the software and tools available to them. Even if all recommendations within this report are followed, incidents will continue to happen. However, if organizations implement suggestions made within the report, it will help to reduce the number of incidents that occur, and as has been seen in previous research, the costs incurred to the organizations because of these incidents.⁶

⁶ For more information see the ICAMP study.
http://educause.edu/content.asp?page_id=666&ID=CSD2814&bhcp=1f

Appendix A: CIFAC Instrument

COMPUTER INCIDENT FACTOR ANALYSIS AND CATEGORIZATION

Gerald R. Ford School of Public Policy
The University of Michigan
712 Oakland Street, Room 159
Ann Arbor, MI 48104-3021

734-615-9595 o
734-998-6688 f
cifac.staff@umich.edu

Name _____

Institution _____

Interviewer VR / MB 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 **EXISTANCE** 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: *(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 _____

19. In **CAUSING** this incident to happen, how important was **ACCIDENTAL** or **CARELESS** behavior of the following: *(1) not at all (2) somewhat (3) quite (4) extremely*

IT managers
faculty
students

IT Staff
non-IT Staff
authorized or permitted external users
unauthorized external users
other _____

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

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

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

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

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

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

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

23. Overall, how **EFFECTIVE** were these **PROCEDURES**?

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

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

25. 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 _____

26. 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
27. Is there anything **ELSE** you would like to **SHARE** with us about this incident or its management

INSTITUTIONAL DEMOGRAPHICS

28. 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
29. 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*
30. 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
31. 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
32. 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 B: Sample of 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

Rated: "Systems" incident by the CIFAC respondent

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

Virus outbreak

Rated: "People" incident by the CIFAC respondent

We have a technical measure in place to filter our mail for viruses. Despite this, a virus came in as a .zip attachment. Not only did you have to open the zip to see what files were in it, but also open the file which the instructions said to do. The text in the zip gave these instructions. There were a bunch of spaces so that when you double clicked on this it activated the virus. We update the antiviral on all of the PCs and the servers, every hour. We started getting some calls from the help desk which indicated that probably some virus was going on. Immediately we started blocking .zip files. We do security updates regularly and our users have heard about .zip files, but they don't always remember. We had 20 people infected before we could get on it.

Time Server

Rated: "Data" incident by the CIFAC respondent

The server that is used as our time server on our network. It is the server that controls the time. The utility that you change the time. The window that you use to change the time was open. A non-technical staff individual responsible for changing back-up tapes dismissed the window without looking at it and it reset the time 4 months ahead, which reset the time on all the other servers to reset. Transaction time on SQL servers, problems with email. It required a lot of staff time to control and we had to manually had to run SQL scripts to correct the transaction.

Malicious employee action

Rated: "People" incident by the CIFAC respondent

We had an employee dump soda on a switch/hub and that brought down the network at the remote office. It ruined the hub and took down the ability of that location to connect to the network and fried the motherboards on 15 computers. Individual had to physically go to the server closet and poured the pop on the switch intentionally

Virus outbreak

Rated: "Systems" incident by the CIFAC respondent

On the XP machines, updates were not applied to machines because they are locked. A virus slipped through and promulgated through the XP machines and caused them to lock. At end of reporting period, numerous machines were freezing and sending it on. Containment was a nightmare. Virus came from an outside email source. Dispatched technicians to control and lock down the machines and update them. Educated the instruction staff to identify the virus until IT staff could install patches. Isolate and update o/s. Exploiting weakness in MS Windows XP. contained within one v-LAN

Appendix C: Frequency Tables for Differences Between the Samples

1. Increased personnel resources for prevention (p=0.0043);

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	54	41	13	2	110
% within Sample	49.09%	37.27%	11.82%	1.82%	100.00%
Acad	119	96	60	40	315
% within Sample	37.78%	30.48%	19.05%	12.70%	100.00%
Combined	173	137	73	42	425
% within Sample	40.71%	32.24%	17.18%	9.88%	100.00%

2. Increased audit procedures for prevention (p=0.0114);

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	26	36	30	18	110
% within Sample	23.64%	32.73%	27.27%	16.36%	100.00%
Acad	114	55	73	68	310
% within Sample	36.77%	17.74%	23.55%	21.94%	100.00%
Combined	140	91	103	86	420
% within Sample	33.33%	21.67%	24.52%	20.48%	100.00%

3. Existence of backup for prevention (p=0.0026);

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	62	20	14	14	110
% within Sample	56.36%	18.18%	12.73%	12.73%	100.00%
Acad	226	23	15	46	310
% within Sample	72.90%	7.42%	4.84%	14.84%	100.00%
Combined	288	43	29	60	420
% within Sample	68.57%	10.24%	6.90%	14.29%	100.00%

4. Existence of logging for prevention (p=0.0122)

Logging Prev	Not At All	Somewhat	Quite	Extremely	Total
CNFP	26	36	29	19	110
% within Sample	23.64%	32.73%	26.36%	17.27%	100.00%
Acad	115	51	74	68	308
% within Sample	37.34%	16.56%	24.03%	22.08%	100.00%
Combined	141	87	103	87	418
% within Sample	33.73%	20.81%	24.64%	20.81%	100.00%

5. Existence of analysis of logs for preventing incidents (p=0.0179)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	43	21	25	21	110
% within Sample	39.09%	19.09%	22.73%	19.09%	100.00%
Acad	115	65	65	65	310
% within Sample	37.10%	20.97%	20.97%	20.97%	100.00%
Combined	158	86	90	86	420
% within Sample	37.62%	20.48%	21.43%	20.48%	100.00%

6. Increased requirements for use of personal information for prevention (p=0.0013)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	75	20	11	4	110
% within Sample	68.18%	18.18%	10.00%	3.64%	100.00%
Acad	171	41	31	63	306
% within Sample	55.88%	13.40%	10.13%	20.59%	100.00%
Combined	246	61	42	67	416
% within Sample	59.13%	14.66%	10.10%	16.11%	100.00%

7. Increased configuration requirements for mainframe and server software for prevention (p=0.0003)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	30	30	37	13	110
% within Sample	27.27%	27.27%	33.64%	11.82%	100.00%
Acad	153	52	52	52	309
% within Sample	49.51%	16.83%	16.83%	16.83%	100.00%
Combined	183	82	89	65	419
% within Sample	43.68%	19.57%	21.24%	15.51%	100.00%

8. Increased configuration requirements for networks to prevent incidents (p=0.0255)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	38	28	30	14	110
% within Sample	34.55%	25.45%	27.27%	12.73%	100.00%
Acad	160	56	55	34	305
% within Sample	52.46%	18.36%	18.03%	11.15%	100.00%
Combined	198	84	85	48	415
% within Sample	47.71%	20.24%	20.48%	11.57%	100.00%

9. Increased configuration requirements for desktop software to prevent incidents (p=0.0468)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	65	22	10	12	109
% within Sample	59.63%	20.18%	9.17%	11.01%	100.00%
Acad	173	36	51	48	308
% within Sample	56.17%	11.69%	16.56%	15.58%	100.00%
Combined	238	58	61	60	417
% within Sample	57.07%	13.91%	14.63%	14.39%	100.00%

10. Lack of auditing procedures was seen as important cause of incidents (p=0.0019)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	38	41	23	8	110
% within Sample	34.55%	37.27%	20.91%	7.27%	100.00%
Acad	164	54	53	37	308
% within Sample	53.25%	17.53%	17.21%	12.01%	100.00%
Combined	202	95	76	45	418
% within Sample	48.33%	22.73%	18.18%	10.77%	100.00%

11. Lack of requirements for the use of personal information as a cause (p=0.0195).

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	91	11	4	4	110
% within Sample	82.73%	10.00%	3.64%	3.64%	100.00%
Acad	209	39	19	39	306
% within Sample	68.30%	12.75%	6.21%	12.75%	100.00%
Combined	300	50	23	43	416
% within Sample	72.12%	12.02%	5.53%	10.34%	100.00%

12. Lack of configuration requirements of mainframe and server software as a cause (p=0.0373)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	45	31	18	16	110
% within Sample	40.91%	28.18%	16.36%	14.55%	100.00%
Acad	181	48	41	34	304
% within Sample	59.54%	15.79%	13.49%	11.18%	100.00%
Combined	226	79	59	50	414
% within Sample	54.59%	19.08%	14.25%	12.08%	100.00%

13. Lack of configuration requirements for desktop hardware as a cause of incidents (p=0.0072)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	106	1	3	0	110
% within Sample	96.36%	0.91%	2.73%	0.00%	100.00%
Acad	268	31	3	4	306
% within Sample	87.58%	10.13%	0.98%	1.31%	100.00%
Combined	374	32	6	4	416
% within Sample	89.90%	7.69%	1.44%	0.96%	100.00%

14. Lack of analysis of logs as a cause of incidents (p=0.0219)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	57	33	17	3	110
% within Sample	51.82%	30.00%	15.45%	2.73%	100.00%
Acad	189	47	41	28	305
% within Sample	61.97%	15.41%	13.44%	9.18%	100.00%
Combined	246	80	58	31	415
% within Sample	59.28%	19.28%	13.98%	7.47%	100.00%

15. The number of people affected in an incident as a stimulus to action (p=0.0496)

	Not At All	Somewhat	Quite	Extremely	Total
CNFP	10	28	32	40	110
% within Sample	9.09%	25.45%	29.09%	36.36%	100.00%
Acad	66	56	68	122	312
% within Sample	21.15%	17.95%	21.79%	39.10%	100.00%
Combined	76	84	100	162	422
% within Sample	18.01%	19.91%	23.70%	38.39%	100.00%

16. Number of Users the IT System Supports ($p < .001$)

users	1	2	3	4	5	6	7	Total
CNFP	6	9	1	6	9	5	6	42
% within Sample	14.29%	21.43%	2.38%	14.29%	21.43%	5.43%	6.52%	100.00%
Acad	0	0	2	11	26	36	11	86
% within Sample	0.00%	0.00%	2.33%	12.79%	30.23%	41.86%	12.79%	100.00%
Combined	6	9	3	17	35	41	17	128
% within Sample	4.69%	7.03%	2.34%	13.28%	27.34%	32.03%	13.28%	100.00%

17. To what extent IT systems are managed from a central office ($p < 0.001$).

Centrality	Not At All	Somewhat	Quite	Extremely	Total
CNFP	0	9	14	19	42
% within Sample	0.00%	21.43%	33.33%	45.24%	100.00%
Acad	3	34	27	20	84
% within Sample	3.57%	40.48%	32.14%	23.81%	100.00%
Combined	3	43	41	39	126
% within Sample	2.38%	34.13%	32.54%	30.95%	100.00%

18. The existence of norms that require IT personnel to involve attorneys in handling incidents.
($p=0001$)

	No	Yes	Total
CNFP	17	25	42
% within Sample	40.48%	59.52%	100.00%
Acad	17	65	82
%within Sample	20.73%	79.27%	100.00%
Combined	34	90	124
% within Sample	27.42%	72.58%	100.00%

19. The existence of norms that require IT personnel to involve law enforcement in handling incidents

	No	Yes	Total
CNFP	23	19	42
% within Sample	54.76%	45.24%	100.00%
Acad	20	62	82
%within Sample	24.39%	75.61%	100.00%
Combined	43	81	124
% within Sample	34.68%	65.32%	100.00%

Appendix D: Variables Clusters for Each Factor

This Appendix contains a listing of the variables that cluster together making up each of the factors in the CIFAC study. The Factors are shown below for the Academic Sample and then for the Corporate/NFP sample, first for the cause factors and then for the prevention factors. Each factor has been named according to the variables clustered within it.

Cause Factors—Academic Sample

Factor 1-“Training/Education & Requirements: IT managers/staff”

Variables Cluster:

- ◆ Lack or deficiency of education for IT managers
- ◆ Lack or deficiency of education for IT staff
- ◆ Lack of procedures for audit
- ◆ Lack or deficiency of requirements for IT managers
- ◆ Lack or deficiency of requirements for IT staff
- ◆ Accidental behavior of IT staff
- ◆ Accidental behavior of IT staff

Factor 2-“Training/Education & Requirements: Non-IT staff”

Variables Cluster:

- ◆ Lack or physical security resources
- ◆ Lack or deficiency of education for non-IT staff
- ◆ Lack of requirements for the use of personal information
- ◆ Lack of requirements for non-IT staff
- ◆ Lack of requirements for the use of institutional resources
- ◆ Lack of identification, authentication, and authorization mechanisms
- ◆ Lack or deficiency of policies
- ◆ Accidental behavior of non-IT staff
- ◆ Abusive behavior of non-IT staff

Factor 3-“Resources and Configuration Requirements: Hardware, software, networks”

Variables Cluster:

- ◆ Lack or deficiency of hardware resources
- ◆ Lack or deficiency of software resources
- ◆ Lack or deficiency of network resources
- ◆ Lack or deficiency of procedures for networks
- ◆ Lack of configuration requirements for networks
- ◆ Lack of configuration requirements for hardware

Factor 4-“Procedures for incident response”

Variables Cluster:

- ◆ Lack or deficiency of personnel resources
- ◆ Lack or deficiency of education for incident investigators
- ◆ Lack of procedures for incident response
- ◆ Lack or deficiency of documentation for systems

Factor 5-“Management Procedures: Detecting, & Responding-External Users”

Variables Cluster:

- ◆ Lack of procedures for audit

- ◆ Lack or deficiency of knowledge required for authorized external users
- ◆ Lack of configuration requirements for desktop software
- ◆ Lack of procedures for logging
- ◆ Lack of procedures for analysis of logs
- ◆ Accidental behavior of authorized external users
- ◆ Accidental behavior of unauthorized external users
- ◆ Abusive behavior of unauthorized external users

Factor 6–“Management Procedures: Recovery”

Variables Cluster:

- ◆ Lack of procedures for backup
- ◆ Lack of procedures for documentation of systems
- ◆ Lack of configuration requirements for mainframes and servers
- ◆ Lack of configuration requirements for mainframe hardware
- ◆ Lack of backup

Cause Factors- Corporate/NFP Sample

Factor 1-“Training/Education & Requirements: IT managers/staff”

Variables Cluster:

- ◆ Lack or deficiency in personnel resources
- ◆ Lack or deficiency of education for IT managers
- ◆ Lack or deficiency of education for IT staff
- ◆ Lack of configuration requirements for networks
- ◆ Lack of procedures for incident response
- ◆ Lack of procedures for documenting systems
- ◆ Lack or deficiency of requirements for IT managers
- ◆ Lack or deficiency of requirements for IT staff
- ◆ Accidental behavior of IT staff
- ◆ Accidental behavior of IT staff
- ◆ Lack or deficiency of documentation
- ◆ Lack or deficiency of policies

Factor 2-“Management Procedures: Detection”

Variables Cluster:

- ◆ Lack or deficiency of education for incident investigators
- ◆ Lack of procedures for audit
- ◆ Lack of procedures for network
- ◆ Lack of configuration requirements for networks
- ◆ Lack of configuration requirements for mainframe software
- ◆ Lack of identification authentication, authorization processes
- ◆ Lack of logging
- ◆ Lack of analysis of logs
- ◆ Abusive behavior of non-IT staff

Factor 3-“Management Procedures: Response and Recovery”

Variables Cluster:

- ◆ Lack of configuration requirements for hardware
- ◆ Lack or deficiency of education for incident investigators
- ◆ Lack of procedures incident response
- ◆ Lack of procedures for backup
- ◆ Lack of procedures for documenting systems
- ◆ Lack of configuration requirements for mainframe hardware
- ◆ Lack of backup

Factor 4-“Training/Education & Requirements: Non-IT staff”

Variables Cluster:

- ◆ Lack or physical security resources
- ◆ Lack or deficiency of education for non-IT staff
- ◆ Lack of requirements for non-IT staff
- ◆ Lack of requirements for the use of institutional resources
- ◆ Lack or deficiency of policies
- ◆ Accidental behavior of Non-IT staff

Factor 5-“Training/Education: External Users”

Variables Cluster:

- ◆ Lack of knowledge required prior to use for external users
- ◆ Accidental behavior of unauthorized external users
- ◆ Accidental behavior of authorized external users
- ◆ Abusive behavior of unauthorized external users

Factor 6-“Resources & Configuration Requirements: Software and Networks”

Variables Cluster:

- ◆ Lack of physical security resources
- ◆ Lack of software resources
- ◆ Lack of network resources
- ◆ Lack of requirements for the use of personal information
- ◆ Lack of configuration requirements for desktop software
- ◆ Lack of configuration requirements for hardware

Prevention Factors-Academic Sample

Factor 1-“Management Procedures: Detection & Response”

Variables Cluster:

- ◆ Increased or improved procedures for network management
- ◆ Increased or improved procedures for incident response
- ◆ Increased or improved procedures for documenting systems
- ◆ Increased or improved procedures for audit
- ◆ Increased or improved identification, authentication, and authorization mechanisms
- ◆ Increased or improved logs
- ◆ Increased or improved analysis of logs

Factor 2-“Training/Education: External Users & Non-IT staff”

Variables Cluster:

- ◆ Increased or improved education for Non-IT staff
- ◆ Increased or improved education for authorized external users
- ◆ Higher level of knowledge required prior to use of systems for authorized external users
- ◆ Higher level of knowledge required prior to use of systems for non-IT staff

Factor 3-“Management Procedures for Software”

Variables Cluster:

- ◆ Increased or improved requirements for access control
- ◆ Increased or improved procedures for detecting software bugs
- ◆ Increased or improved procedures for configuring for software
- ◆ Increased or improved configuration requirements for mainframe software
- ◆ Increased or improved configuration requirements for software

Factor 4-“Training/Education & Requirements: IT managers & staff”

Variables Cluster:

- ◆ Increased or improved education for IT managers
- ◆ Increased or improved education for IT staff
- ◆ Promulgated policies
- ◆ Increased or improved requirements for IT managers
- ◆ Increased or improved requirements for IT staff

Factor 5-“Management Procedures: Recovery”

Variables Cluster:

- ◆ Increased or improved procedures for backup
- ◆ Increased or improved procedures for documenting systems
- ◆ Increased or improved procedures for backup
- ◆ Increased or improved documentation of systems
- ◆ Increased or improved configuration requirements for mainframe/server hardware

Factor 6-“Configuration Requirements: Networks & Desktops”

Variables Cluster:

- ◆ Increased or improved network resources
- ◆ Increased or improved procedures for network management

- ◆ Increased or improved configuration requirements for networks
- ◆ Increased or improved configuration requirements for software
- ◆ Increased or improved configuration requirements for hardware

Factor 7-“Resources: Hardware, software, personnel”

Variables Cluster:

- ◆ Increased or improved personnel resources
- ◆ Increased or improved hardware resources
- ◆ Increased or improved software resources
- ◆ Increased or improved configuration requirements for mainframe/server hardware

Factor 8-“Access Control Requirements: Policy”

Variables Cluster:

- ◆ Increased or improved access control resources
- ◆ Increased or improved physical security resources
- ◆ Increased or improved policies
- ◆ Increased or improved requirements for the use of personal information
- ◆ Increased or improved requirements for the use of institutional resources

Prevention-Corporate/NFP Sample

Factor 1-“Training/Education & Requirements: IT managers/staff and external users”

Variables Cluster:

- ◆ Lack or deficiency of education for authorized external users
- ◆ Lack or deficiency of education for IT managers
- ◆ Lack or deficiency of education for IT staff
- ◆ Lack of requirements for IT managers
- ◆ Lack of requirements for IT staff
- ◆ Lack of knowledge required prior to use of systems for authorized external users

Factor 2-“Magement Procedures: Detection, Response & Recovery”

Variables Cluster:

- ◆ Lack of hardware resources
- ◆ Lack of procedures for response
- ◆ Lack of procedures for backup
- ◆ Lack of procedures for documentation of systems
- ◆ Lack of procedures for audit
- ◆ Lack of existence of backup
- ◆ Lack of existence of documentation of systems
- ◆ Lack of existence of promulgated policies
- ◆ Lack or deficiency of education for authorized external users

Factor 3-“Training/Education: External Users & Non-IT staff”

Variables Cluster:

- ◆ Lack or deficiency of education for authorized external users
- ◆ Lack or deficiency of education for Non-IT staff
- ◆ Lack of existence of promulgated policies
- ◆ Lack of requirements for the use of institutional resources
- ◆ Lack of identification, authentication, and authorization mechanisms
- ◆ Lack of knowledge required prior to use for authorized external users
- ◆ Lack of knowledge required prior to use for non-IT staff

Factor 4-“Management Procedures: Software”

Variables Cluster:

- ◆ Lack of personnel resources
- ◆ Lack of software resources
- ◆ Lack of requirements for detecting software bugs
- ◆ Lack of procedures for configuration of software
- ◆ Lack of configuration requirements for mainframes & servers
- ◆ Lack of configuration requirements for software

Factor 5-“Detection Procedures: Logging”

Variables Cluster:

- ◆ Lack or physical security resources
- ◆ Lack of existence of logging
- ◆ Lack of existence of analysis of logs

Factor 6-“Management Procedures: hardware, software, networks”

Variables Cluster:

- ◆ Lack of hardware resources
- ◆ Lack of software resources
- ◆ Lack of network resources
- ◆ Lack of configuration requirements for desktop hardware
- ◆ Lack of configuration requirements for mainframe & server hardware

Factor 7-“Access Control Requirements”

Variables Cluster:

- ◆ Lack of access control resources
- ◆ Lack of physical security resources
- ◆ Lack of existence of identification, authentication, authorization resources
- ◆ Lack of requirements for the use of personal information

Factor 8-“Management Procedures: Networks”

Variables Cluster:

- ◆ Procedures for network management
- ◆ Configuration requirements for networks

Appendix E: 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 violators. 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