FINAL REPORT

Incident Cost Analysis and Modeling Project

A Report from the CIC Security Working Group to the CIC Chief Information Officers

DEDICATION

Scott Ziobro

September 27, 1971 - September 22, 1997

Scott Ziobro contributed two important things to this project: his mind and his spirit. It was his mind, his exceptional care and attention to detail, that created the framework for this project. And it was his spirit that kept him coming back to the office, always with that same brave, knowing smile.

Scott Ziobro passed away on September 22, 1997, as a result of a brain tumor. He was 25 years old. This tumor, though it may have affected his ability to speak and to write, never affected his truly gifted mind. And this tumor, though it made him tire before his years and eventually took him from us too soon, never once took away his amazingly strong spirit.

We have been inspired by Scott's gifted mind to produce the same quality research that Scott always demanded of himself. We have depended heavily on Scott's spirit to get us through the darkest of days. Without these two things, this project would not be where it is today.

Each of us had a unique relationship with Scott. We will always cherish our memories of him and are thankful that he was a part of our lives.

This project is dedicated to Scott Ziobro. A gifted mind, a loving spirit.

CREDITS

Project Staff

Project Director
Virginia Rezmierski, Ph.D.
Director Office of Policy Development and Education
University of Michigan

Stephen Deering, M.P.P.
Research Associate
University of Michigan

Amy Fazio, M.S.I.
Research Associate
University of Michigan

Scott Ziobro, M.P.P., deceased
Risk Management Analyst
University of Michigan

Project Advisory Board

George Cubberly
Assistant Risk Manager
Office of the Associate Vice President for Finance
Department of Risk Management
The University of Michigan

Kathy Kimball, M.S.
Security Director
Computer Information Systems
Pennsylvania State University

Eugene Spafford, Ph.D.
Professor of Computer Sciences
Director, COAST Project and Laboratory
Purdue University

Larry Stephens, AIC, EPCU, ARM
Director of Risk Management
Department of Risk Management
Indiana University

CONTENTS

FIGURES

TABLES

ACKNOWLEDGMENTS

We would like to thank the staff of the Office of Policy Development and

Education at the University of Michigan for their continued input and support, especially our editor, Theresa Hofer; David Nesom for technical advice; and Gwen Reichbach for further content editing. We would also like to thank Jon Leonard, technical advisor for ICAMP; Edward Gramlich; and Ruth Kallio.

We would like to give special thanks to the Committee on Institutional Cooperation Security Working Group for its advice and support, which remained constant throughout the project.

Additional thanks goes to the ICAMP Advisory Board Members for their valuable input and assistance, as well as to all individuals from the CIC institutions who helped us gather the necessary data for the incidents included in this report.

EXECUTIVE SUMMARY

The purpose of the Incident Cost Analysis and Modeling Project (ICAMP) was to develop a methodology for understanding the factors that influence the occurrence and costs of incidents in computing environments. It also sought to provide a sense of the magnitude of overall loss to universities from particular incidents related to information technology (IT).

A nonrandom sample of 30 IT-related incidents from the participating Committee on Institutional Cooperation (CIC) institutions was identified and analyzed. In these 30 incidents, we found the following:

- 210 employees were involved in incident investigation and/or resolution.
- 9,078 employee hours were devoted to incident investigation and/or resolution.
- An estimated 270,805 computer and network users were affected by the incidents.
- Calculated costs for the 30 incidents totaled $1,015,810.

The ICAMP study:

- Established for the first time an estimate of the actual costs of particular IT incidents.
- Opened channels for sharing information about IT incidents.
- Provided a sample of incident types, as well as a template and methodology for IT staff to calculate the costs of incidents on their own campuses.
- Began the process of identifying factors that appear to affect the occurrence and costs of incidents.
- Identified the unquantifiable effects of individual incidents.
- Established a framework and objectives for future study.

The number of incidents occurring on the campuses appears to be increasing. It is uncertain whether this apparent increase is due to more incidents or a higher rate of incident discovery. The sample of incidents included in this study is but one segment of those which occur each year on campuses. The range of incident types is wider than those discovered in the scope of this project. Managing the risks and liabilities associated with IT-related incidents is a real and existing challenge for university administrators. The CIC Security Officers and Chief Information Officers (CIOs) recognized the need for more information and began the process of discovery. The project showed that before risks can be more fully understood and specific management recommendations formulated, more needs to be done. Specific recommendations include the following:

1. Develop a more formal method of incident reporting on each campus.
2. Establish agreement on specific incident types to be analyzed.
3. Continue developing a predictive cost analysis model.

4. Improve collaboration between data stewards, risk managers, and technologists.

BACKGROUND

The Problem

The implementation and rapid evolution of information technology (IT) resources at universities has increased the number of security and risk management issues of concern to institutions of higher education. Security processes, both physical and electronic, which were familiar in mainframe environments are no longer suitable in more distributed computing environments. Individuals now handling the distributed services are at differing levels of sophistication regarding the technology, laws, and ethics governing data security. The need to guarantee a viable computing environment requires the education of its keepers, an awareness of the key features of data security, hardware maintenance, software compatibility, and an understanding of the implications of physical theft, infrastructure failure, and employee incompetence or inexperience.

Given the number of incidents occurring at a typical university today, one might expect executive officers of colleges and universities to be pressing staff for increased security and security education. Too often, however, executive officers are unaware of the vulnerabilities, lack information about actual incidents, and are unsure of how to identify the factors that influence the occurrence and costs of incidents.

The absence of data, the press of conflicting demands for fiscal resources, and an environment of rapid technological change can combine to create a climate in which administrators prefer not to hear about more problems. As a result, a tendency can develop to underestimate the frequency with which incidents occur or to consider individual incident costs as insignificant when compared with the institution's overall expenses.

To take such an approach, however, leaves an institution open to the possibility of serious financial liabilities. A single incident may cost only $2,000. If, however, that same type of incident is repeated at a university 60 times during a month or year, then costs to the university are increased significantly. Without accurate information about the costs and frequency of typical incidents, it is impossible for those concerned with overall campus budgets and expenses to accurately assess and manage IT-related risks.

This study sought to begin the process of incident data gathering and analysis and to raise awareness and discussion levels by addressing one of these needs: the need for a model for assessing and analyzing the costs of IT-related incidents. The current study did not seek to provide frequency data, although we know that the small sample gathered is but a tiny fraction of incidents occurring on campuses.

Need for Costing Model and Cost Analysis

Why should someone be concerned about IT incidents in a university setting? What are the explicit and implicit implications in terms of dollars, time, and user satisfaction?

Risk management personnel on most campuses focus their cost/benefit analysis efforts on known risks such as floods, fires, and legal liability, for which insurance may be obtained to reduce vulnerabilities. To date, few have focused much attention on the risks in the information technology and information resource area. While risk managers have historically insured against the loss of information technology hardware, they are less informed on the potential losses from, for example, data disclosure, hacker attacks, and denial of service attacks. University risk managers who have tried to look at IT-related risks have found that data most often exist for corporate environments, while little exists for academic environments. Without relevant data, risk managers and executive officers are hampered in understanding the types of incidents that occur, their mitigating factors, and the costs that are associated with them. As a result, a university's ability to plan proactively in IT policy areas is less than ideal.

The ICAMP Project

The purpose of the Incident Cost Analysis and Modeling Project (ICAMP) is to develop a methodology for understanding the factors that influence the occurrence and costs of incidents in academic computing environments, and to provide a sense of the magnitude of overall loss to universities from particular information technology incidents. To that end, this project is as much a qualitative discussion of the issues affecting IT incidents in universities as it is a quantitative look at the costs of the incidents we investigated. Identification of the relevant factors in university IT incidents will help managers and executive officers isolate points of intervention for reducing losses. The quantitative aspects of the study will begin to shed light on real losses universities are already experiencing and will continue to experience in the future if action is not taken.

The ICAMP model for understanding academic IT incidents is not meant, as it currently stands, to be statistically predictive of incident costs. Rather, it provides anecdotal evidence that administrators can use to assist in policy decisions. As such, the study makes no claims of having collected a random sample of incidents across universities. Randomness is not a feasible option for this study because there is no reliable data on the frequency with which incidents occur in academic environments. To make the model statistically predictive, an effort should be made to gather such statistics in future studies.

Moreover, all incidents were supplied by individuals employed in IT organizations, who may be exposed to different types of incidents than those employed in other departments of the universities and colleges. In the situations for which the data are available, the figures are necessarily a function of the reporting mechanisms in place. Hence, they can be considered only a lower bound on the true occurrence of incidents, not necessarily reflecting actual occurrence rates, as incidents are generally underreported.

IT incidents occur in infinite combinations of staff levels, departments, data and hardware losses, and lost user time. The relevance of the cost data gathered from particular incidents across universities, schools, and departments will depend in large part on the incident type and environmental factors, such as salary levels and employee competence. Incidents will never occur the same way twice. The factors that influence costs, the manner in which incidents are handled, and the information gleaned from our discussions with incident handlers, however, are transferable across institutions. The discussion of the incidents in this project should provide some insight into these issues.

Leveraging Campus Expertise and Information

College and university personnel know that they have these vulnerabilities on their campuses. They struggle with how to inform executive officers, provide them with information, and manage the risks. They ask, "Should we put more money into security, insurance, and education? Or should we simply keep our heads down and take our chances?"

This project began to gather the expertise and knowledge that exists on these campuses and assembled it into one cohesive information base. This project sought to:

- Increase the sharing of incident information and opens communication about incidents
- Gather and detail incidents from all participating universities
- Work with the campus security representatives to identify variables and levels of data sensitivity to which costs can be assigned

- Analyze costs of the incidents
- Develop materials to increase the awareness of risk management personnel and other managers
- Develop a methodology for understanding and investigating IT incidents' cost parameters

Approval History

In February 1997, the Committee on Institutional Cooperation Chief Information

Officers (CIC-CIOs) approved funding for ICAMP. Preliminary project work began on March 15, 1997, at the University of Michigan's Office of Policy Development and Education under the leadership of the late Scott Ziobro, M.P.P. Stephen Deering, M.P.P., and Amy Fazio, M.S.I., continued his work. The director of the project was Virginia Rezmierski, Ph.D., Director of the Office of Policy Development and Education.

Project Objectives

The specific deliverables for this project included the following:

1. A survey instrument for consistent information gathering regarding security incidents on campuses. The instrument includes a general conceptual framework of variables to which costs and data sensitivity levels for analyzing incidents may be attached.
2. A sample list of incidents that have occurred at several universities, categorized where possible into the conceptual framework.
3. A written description of each incident (minus personal or campus identifying information), the levels of sensitivity involved, and some of the cost factors and estimates that might be applied.
4. Information regarding existing non-corporate IT risk management cost analysis models.
5. The foundation for a cost analysis model for calculating risks using incident details from the university where the incident occurred.

METHODOLOGY

Search for Literature and Existing Models

The ICAMP staff and university risk managers conducted searches for literature and existing models to assist in the ICAMP model development. Significant literature exists on computer-based risks. Nearly all of it, however, falls into two categories: literature that is very technically specific, prescribing very detailed solutions for very specific problems; or literature that is so general that it does little more than introduce the reader to the concept of risk.

In terms of incident cost analysis, we found very few examples of predictive cost models; the few we found were created by profit-seeking firms. Although we were able to obtain written descriptions of their methodologies, the cost modeling packages were too expensive to purchase and, therefore, could not be analyzed more thoroughly. In addition, assuming that information at a university is generally intended to be more accessible than information at a private firm, a private-sector cost model would not necessarily be appropriate for a university computing environment.

Three software-based cost modeling packages relevant to the ICAMP project are described below.

- **BDSS (Bayesian Decision Support System):** This software package gathers information on institutional resources and assigns cost risks to particular assets using a vendor-provided database and Bayes' Theorem to address uncertainty in probabilities. This statistical software package is relevant in terms of predicting costs from identified risks, but it was unclear as to whether the model allowed for the flexibility in the types of IT incidents that we desired. Furthermore, the data required to use the model effectively is not currently available at university-level systems.

- **CRITI-CALC:** CRITI-CALC uses a loss expectancy algorithm to quantify risk exposure for identified computer applications. The software calculates the costs of recovery and back-up, loss potential, and optimum off-site recovery based on scenario analysis of in place safeguards. Again, this model, while predictive, was not inclusive enough for the types of incidents we wanted to include in our model. It did, however, at least qualitatively, provide a foundation for the types of issues the ICAMP model should address.

- **SOS (Security On-line System):** SOS is a tool designed to estimate potential loss from specific IT incidents based on known risks and occurrence probabilities. Users can use the system risk profiles generated by the software's processes to minimize computer risks and potential loss. This modeling package is not quantitatively appropriate for a university setting because the risks and probabilities of incident occurrence have not been identified fully.

In the ICAMP study, we have attempted to begin developing a predictive cost analysis model that can be used by universities with information that is already typically available. The models described above are not necessarily helpful to universities today because the level of data required to use them effectively is simply not available. However, as data reporting becomes more centralized and standardized, we would expect that further development of the ICAMP model would result in a methodology similar to the ones currently used in the private sector. In qualitative terms, the issues of risk factor identification, need for occurrence probabilities, and frequency data as revealed by existing models have been considered and should be pursued in future research.

Definition of an Incident

This study sought to gain insight into what IT staff themselves felt were incidents. Therefore, we did not define "incident" in advance, but collected information on any incident that was shared with us by IT staff within participating institutions. Project staff wanted to see if incidents sorted into categories in and of themselves. Hence, we did not limit our gathering to electronic security-related incidents, but included hardware and software theft, infrastructure failure, and non-malicious data loss as well.

Because our primary contacts were security staff, it became obvious early in the data gathering that the identified incidents were skewed towards events involving unauthorized access or attempted unauthorized access by hackers. As the study progressed, however, the incident pool became more diverse and individuals from a wider background began reporting incidents.

As the study progressed, the following definition of "incident" evolved:

> Any event that takes place through, on, or constituting information technology resources that requires a staff member or administrator to investigate and/or take action to reestablish, maintain, or protect the resources, services, or data of the community or individual members of the community.

By the term "information technology resources," we are referring specifically to those resources, both tangible and intangible, that are related to computer systems and networks. The term includes computer hardware and software, peripherals, and the institutions (administration and employees) that are established to operate the systems.

We offer the above definition as a working definition that might be used to narrow the scope of inquiry or filter the types and kinds of incidents one might attempt to analyze in future studies. It is meant to be inclusive enough to accommodate typical IT security incidents (hacker and denial of service attacks), as well as those not typically thought of as IT incidents (physical theft and infrastructure failure). At the same time, the definition as it is presented is intended to exclude those incidents that have marginal relevance to information technology.

Direct vs. Secondary Costs

Cost analyses conducted by university risk managers and auditors typically focus on the costs that result in direct payments from university coffers. Administrators often mistakenly consider these costs as the only costs that result from an IT incident. This approach misrepresents the total costs to the university. There are costs attributable to IT incidents that are less explicit, yet should be considered real or potential costs in terms of loss. These secondary costs are currently unquantifiable.

We hypothesize that unquantifiable secondary costs are often ignored because it is difficult to quantify or establish causal relationships between an incident and its secondary effects. Nonetheless, it is important for IT administrators and university executive officers to be aware of the secondary effects, because they have the potential to be of greater magnitude than the direct effects and result in a much greater total cost.

In the ICAMP study, we have attempted to capture the unquantifiable secondary costs. They include the following:

- **Legal liability:** An IT incident has the potential to create legal liability for an institution. If, for example, personnel data, such as Social Security numbers, phone numbers, or addresses, are stolen or disclosed inadvertently, the real possibility exists of a lawsuit against the university.

- **Diminished reputation:** IT incidents have the potential to slowly deteriorate a university's reputation if its users lose faith in a system's reliability. The level of incoming students, grants, and faculty appointments can be affected over the long term by having a reputation for instability in the area information technology resources and operations.

- **Psychological costs:** Faculty, staff, and students have reported feeling violated by specific IT incidents. Loss of privacy or information disclosure should be considered real costs to the academic computing environment.

University administrators and IT specialists should be wary of the unquantifiable secondary effects of IT incidents when thinking about costs. Accurate estimates of IT incident costs must address the potential or real losses that result from the secondary effects of an incident, as well as the more obvious direct costs.

Procedure For Incident Identification

Incident identification on each CIC campus was done by local system administrators. ICAMP project staff used a systematic procedure to gain access to the campuses. The project director sought authorization directly from each campus's Chief Information Officer (CIO). The CIOs, after authorizing project staff to gather data on their respective campuses, identified the significant staff members from whom data should initially be sought and relayed those names to the ICAMP team. The CIOs then informed their staffs of their participation in the ICAMP project, easing the way for the first contact from the project staff. Following the data gathering and the incident analysis from a given campus, the CIO was sent a preliminary report detailing the incidents from his or her campus.

Procedure for Incident Cost Analysis

To begin the investigative and analytic process, project staff contacted the designated campus staff members, solicited information about available incidents, selected one or two for further discussion, provided the staff with questions that needed to be answered, and established a date for data gathering via a campus visit or phone appointment. Additional relevant campus staff were usually identified during this process and were then involved in further discussion of the incident. Often an incident required follow-up data gathering to clarify particular aspects of the event, gather a piece of needed data, or ask a question when some aspect of the event was omitted. Follow-up data gathering was generally accomplished via electronic mail or telephone.

Assumptions

This section of the report details the assumptions used in gathering data and the manner in which cost variables were treated. This information should be used as a guide for understanding the subsequent incident analyses. For a detailed description of the conventions used in calculating costs, refer to Appendix B.

Assumption 1

We assumed that the information that we received from the people directly involved in an incident was truthful to the best of their knowledge. Other than an occasional log of employee actions, we depended primarily on the person's best recollection of events. We attempted to gather data as close to the incident's occurrence as possible to minimize data loss due to memory lapses. While some measure of error exists when recalling past events, we have no grounds for disputing the information conveyed. If an incident was too old to feasibly gather valid data, it was not included in the study.

Assumption 2

We assumed that the individuals identified to provide data about incidents were appropriate and valuable for the purposes of this study. We recognized, however, that as a result of their association with the information technology organizations of these colleges and universities, they would identify incidents of one type more often than might individuals in non-technology departments. Hence, the sample of incidents has not been randomly selected.

Assumption 3

When quantifying an incident, we did so from a university's perspective. However, we made the assumption that the term "university" implies the entire community of students, faculty, and staff. Thus, costs borne by students, for example, from the inability to complete work as a result of a server crash are considered a real cost to the university and estimated for reporting even though the university may not directly pay out resources. Generally, any quantifiable cost borne by any member of the community as a result of an incident, if we are able to estimate it reasonably, is included in our calculations. Otherwise, the potential or real costs and their implications are described qualitatively in the incident report.

Assumption 4

For the purposes of this study, we concluded our cost analysis when the network, system, LAN, PC, or other environment was returned to its pre-incident condition. The decision of when to close the quantification of an incident is debatable and, in some sense, arbitrary. Often it involves a judgment in terms of natural closure-that is, a judgment of when the incident really ended. In general, we attempted to capture the essence of an incident without carrying it out too far. Therefore, if a security audit or review was stimulated by the event and was performed after the problem had been resolved or the hole closed, it was not included in the cost analysis. For the purposes of this study, we did not consider these additional events and their concomitant costs to be directly related to the cost analysis of the incident.

Assumption 5

There are specific variables common to all incidents that we did not attempt to quantify, unless they presented themselves as inordinately large in proportion to and specifically related to the overall incident. Generally, these variables did not provide any clearer sense of the situation, but would have required a significant commitment to data gathering. Included in this category are office supply costs (such as paper and pens), telephone bills, and costs of secretarial support to the individuals involved.

Assumption 6

We did not include time spent by the researchers of this project as part of the overall costs to a university. Under normal circumstances, an incident would not include an investigation by a separate party; thus, we did not want to skew the results of an incident analysis by including the commitment of the project.

Assumption 7

Incidents exist for which estimating user costs becomes intractable. In the cases where the potential number of users affected by an incident was more than 5,000, we did not attempt to estimate their overall loss. Even in incidents involving a relatively small number of affected users, problems in estimating loss existed. Given the

diversity of users in a university computing environment, it is impossible to responsibly estimate how an average user is affected. In the few cases where this applies, we discussed the potential loss qualitatively, but did not attempt to quantify the loss, choosing instead to make the reader aware of the potentially large losses associated with the user costs.

Limitations of the Study

As noted above, it was not an objective of the study to analyze randomly selected IT-related incidents, although such an objective would be valuable at a later stage of investigation. Neither was it an objective to collect frequency data, although such data are critical to analyzing and projecting overall costs to institutions.

The study also recognized, as previously noted, limitations in trying to calculate the user costs within a networked environment when the number of users affected was large. Knowing these numbers precisely would certainly contribute to understanding the overall costs to institutions and communities. However, even identifying the affected users becomes, in incidents of a large scope, impossible. The mere fact that large scope incidents are occurring and are affecting many users must be carefully considered, even if we were unable to cost analyze these incidents at this stage.

The numbers presented in this study are intended to provide a general sense of data do not represent scientifically collected, randomly sampled, representative data that could be analyzed statistically. The incidents that were gathered were analyzed retrospectively. Yet they provide insight into understanding the costs being experienced by incident handlers, computer users, and the institutions overall. They cannot be ignored because they provide one of the first windows into this area of college and university liability, risk, and loss.

THE ICAMP MODEL DEVELOPMENT

The charge of this project was to help universities better understand the costs and risks of IT incidents. Therefore, the ICAMP team gathered and analyzed a sample of incidents and developed a survey instrument for incident data gathering. From the gathered data, we identified the factors that appear to influence the occurrence of incidents and the factors that appear to influence costs. The ICAMP model includes:

- Factors identified as having the potential to increase the occurrence of incidents, or occurrence factors (OFs)
- Factors identified as having the potential to increase the cost of an incident, or cost factors (CFs)
- Specific cost conventions to be applied to individual incidents and a specific template for data gathering

We address each of these elements in turn.

Factors that Increase the Potential for the Occurrence of Incidents

During this study, we identified several factors that seemed to affect the occurrence of incidents. We present these factors as a beginning list to be addressed as campus personnel think about education and prevention. The factors include the following:

1. **Hacker communities:** Hacker communities enter into systems for many reasons. Some break into systems just for the challenge. Others take a vigilante attitude and hack systems in order to expose vulnerabilities. Some hackers try to damage systems or gather information.

   University systems seem to be especially vulnerable and inviting to the hacker community. Many hackers know that university systems are not as secure as others, often due to a lack of resources. Also, many hackers are aware that universities encourage a sense of openness that is not usually found in the corporate world, and they take advantage of it.

2. **Openness of system(s):** This factor has two aspects, one philosophical, the other physical. Philosophically, academic communities foster openness and the sharing of knowledge; this is a cornerstone of academia. Yet this philosophy can become a problem when carried into the world of information technology. Physically, many systems on campuses are insecure or poorly configured, which contributes to the occurrence of a variety of IT-related incidents.

3. **Training issues:** In several incidents, the low competency level of the personnel seemed to contribute to the occurrence of the incident. Factors affecting competency could include a lack of training and knowledge about the appropriate handling or securing of resources; human error in operations management, perhaps as a result of insufficient or inadequate training; and inadequate supervision.

4. **Policy issues:** In some situations, incidents occurred because policy was totally absent and no standards were set. In other cases, policy existed, but it did not adequately guide personnel or users in appropriate use of technology.

5. **Physical security:** This factor represents inadequate protection of the IT resources against theft. Examples of this factor include unlocked facilities, inadequate inventory systems, inappropriate distribution of access devices, and inadequate levels of protection given the value of the resource.

6. **Hardware/software incompatibility:** This factor affects the occurrence of an incident when, for example, hardware /software compatibility problems contribute directly to a loss.

7. **Hardware/software maintenance:** Maintenance refers to keeping hardware and software at its most appropriate operational and security level. This factor affects the occurrence of an incident when, for example, identified and needed security patches to software have not been installed, or hardware, that by its age and nature can no longer be secured, has not been replaced.

8. **Lack of resources:** Lack of human, physical, and fiscal resources affected the occurrence of many incidents. For example, in a number of incidents the system administrator had already identified a needed tool for securing a machine or recognized the need for additional people to install patches or perform critical security upgrades, but was unable to obtain the needed resource(s) due to funding or hiring constraints. (Note: Hiring constraints included the inability to identify and retain technically skilled employees.)

9. **Failure to comply with directions:** In some cases, although specific guidelines or policies existed, individuals failed to comply with the policies or guidelines, which affected the occurrence of an incident. This factor includes the refusal to follow directions or recommendations for security and communication problems between employee and manager that resulted in inadequate follow-through.

10. **Appropriateness of level of security:** This factor affects the occurrence of an incident when the level of security selected was found inadequate to the level of sensitivity of the resource and resulted in loss. An example of this factor would be inadequate identification and authentication processes for sensitive data.

11. **Appropriateness of use:** In some cases, hardware and/or software was not used for its originally intended purpose. The inappropriate use resulted in a vulnerability that, in turn, resulted in an incident.

12. **Faulty hardware and software:** This factor affects the occurrence of incidents when hardware or software is not working correctly or is not performing according to its expectations. Examples include software bugs or system malfunctions.

Factors that Have the Potential to Increase the Costs of Incidents

Factors were also identified in this study that have the potential to increase the costs of incidents. Specifically, our intent was to identify any relationship between cost levels and the factors that influence them, factors that – all other things being equal – result in higher costs.

1. **Lack of knowledge:** This factor affects costs when the personnel do not know how to handle, investigate, or manage an incident. Such incidents involve lack of direction, planning, and procedures.

2. **Capture vs. closing holes:** This factor, which affects hacking incidents, refers to the decision to either close the existing vulnerabilities in a system or leave them open and launch an investigation with the hopes of capturing the hacker.

3. **No backup for reinstallation:** This factor affects costs when no backups are available for reinstalling systems or documents, or the backups that are available are too old to run on current systems. The lack of usable backups increases costs by increasing the time spent waiting for replacement systems or re-entering data.

4. **Age of systems:** This factor affects the cost of an incident when the age of a system contributes to the cost. Often, if newer, updated equipment was available to use to resolve incidents, considerable time could be saved and costs would not be as high.

5. **Lack of resources:** The lack of human, physical, or fiscal resources needed to resolve an incident can contribute to both the occurrence and the cost of an incident, but they are distinct effects. For example, if an incident needs 20 employees to resolve efficiently, yet the department can afford to pay only five employees, then the incident will take longer to get resolved and costs will rise.

6. **Timing:** The time of the semester, the day, or the year, can affect the number of users affected by an incident or the number of staff required to manage it, thus affecting the costs.

7. **Loss of resources:** This factor directly relates to the number of resources lost and the costs for replacing those resources. These include data loss and the costs of reentry.

8. **Undocumented complex configurations:** This factor affects costs when the lack of a document directly affects an effort and, therefore, the costs for reestablishing the service. When documentation is missing or inadequate, especially in the case of complex or nonstandard configurations, the costs for reconfiguring. the system are significantly affected. This factor also includes situations when documentation was never written down and shared with others, but was contained only in the memory of the system administrator managing the system.

9. **Lack of continuity in staffing and responsibilities:** This factor impacts situations in which the cost of the incident is affected by rapid or uncoordinated personnel changes. Incidents affected by this cost factor were characterized by high turnover and lack of clarity and continuity in passing responsibilities for system management functions from one employee to another, resulting in lost documentation and missed or poorly executed procedures.

10. **Age of incident relative to investigation:** When the investigation of an incident occurred significantly after the incident itself, the amount of effort needed to resolve the incident was increased. In addition, the effects of time on human recall reduced data validity. Data and evidence were also harder to recover; hence, costs had the potential to increase.

11. **Level of personnel involved in investigation:** When individuals of higher rank and salary within an institution, such as attorneys, vice presidents, and media relations personnel, were involved in the investigation of an incident, the incidents costs rose significantly. The use of higher level personnel seemed to be related to the levels of media exposure, potential liability, and perhaps sensitivity of the data involved in the incident.

12. **Coordination of response from external organizations:** An incident's cost tended to be affected when it required the involvement of external organizations due to the coordination effort, the time to resolve the incident, or the need for specific technical consultants. These external organizations included telecommunications corporations, governmental organizations such as the FBI and Secret Service, and equipment vendors.

13. **Lack of monitoring and logging of information:** In some incidents, the system administrator had not monitored, logged, or analyzed information for various machines. In these incidents, this factor increased the time needed to track down the necessary data needed to close the incident and affected the costs of the incident.

14. **Lack of coordination and duplication of effort:** Costs increased when personnel repeated tasks that could have been accomplished more efficiently if coordination had been present.

15. **Software/hardware incompatibility:** The costs of incidents are affected by software/ hardware incompatibility. For example, cost increase when a particular piece of software is needed to resolve an incident, but that software is incompatible with the hardware involved in the incident. Increased costs result from the price of the needed software or from waiting for the appropriate hardware and/or software to arrive in order to resolve the incident.

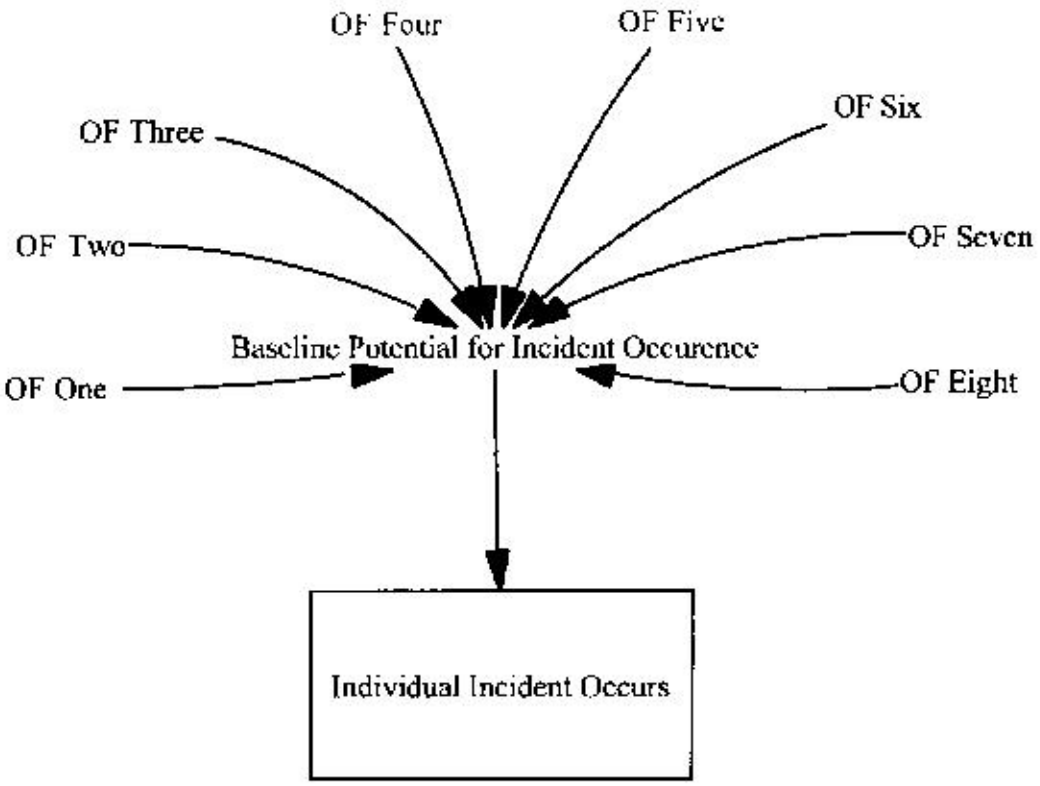
Incident Analysis Template and Costing Conventions

The ICAMP team developed a template for gathering the appropriate incident data. Specific costing conventions and mathematical manipulations were then applied to the data gathered via the template. Both the template and a discussion of the ICAMP costing conventions have been included in Appendix B as a guide for future incident gathering and to assist college and university personnel who wish to analyze their own incident costs.

A Graphical Representation of the Model

The following is a graphical representation of the ICAMP model. Figure 1 shows the way in which incidents occur. Figure 2 shows how a specific incident interacts with its environment to generate costs and how our costing conventions fit into the process.

Figure 1: Impact of Occurrence Factors (OFs) on Incident Occurrence

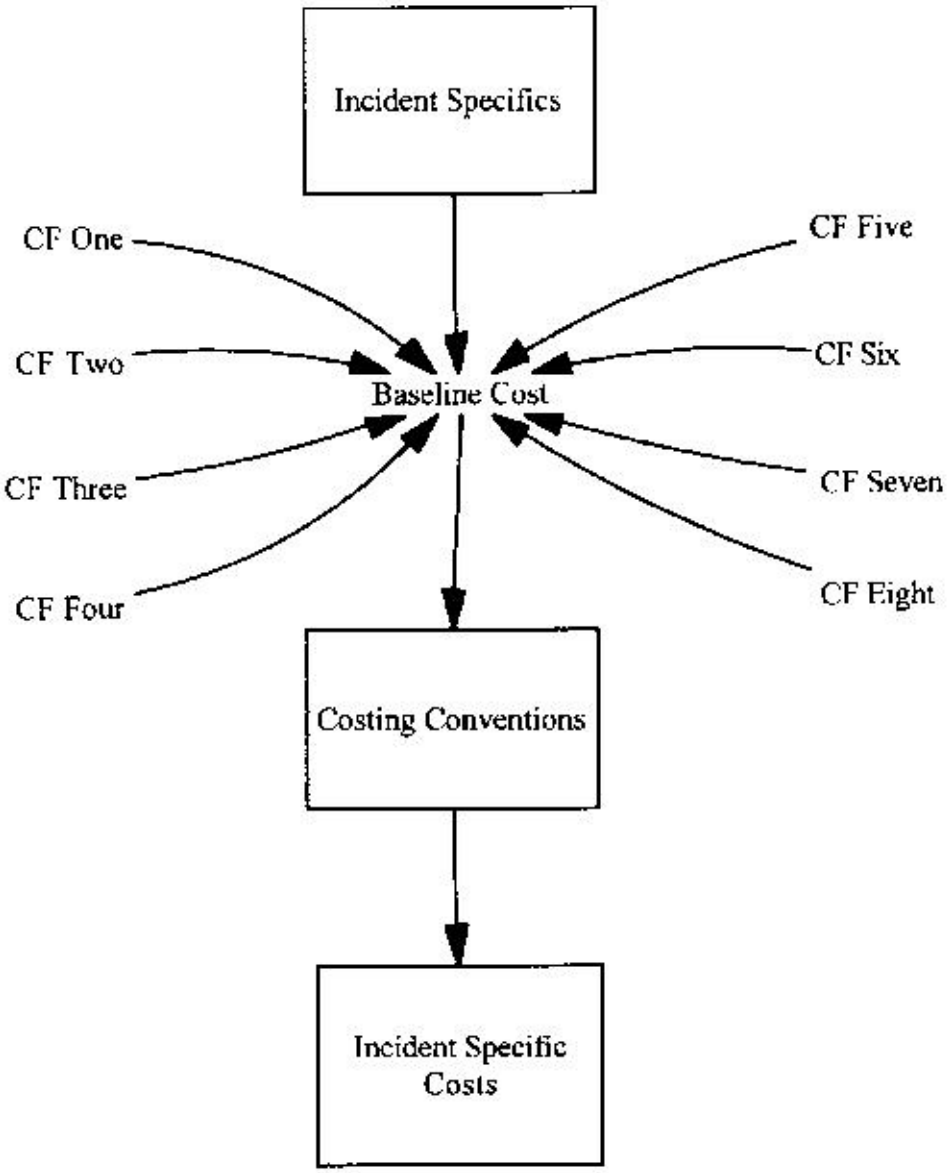


All other things being equal, some potential always exists for an IT incident to occur. Figure 1 represents this as a baseline potential for an IT incident. When the previously identified factors impinge on this baseline, however, the potential for an IT incident seems to increase. In combination, these forces work to provide a window for an incident to occur. The results of this process are specific IT incidents of the types we have studied in this report. Note that the "Factors" variables shown in Figures 1 and 2 represent the factors that were identified from our incident sample, although it is not an exhaustive representation.

Many factors influence the occurrence of IT incidents. Through the ICAMP model, however, we are trying to capture the factors on the margin, those that can presumably be controlled. We cannot, for example, simply rid ourselves of technology in order to prevent IT incidents. But establishing an appropriate level of security can reduce the potential for incidents to occur.

Each IT incident has its own characteristics and unique qualities. These qualities interact with specific factors that appear to increase the costs of incidents. The second part of our model (Figure 2) attempts to explain this interaction.

Figure 2: Impact of Cost Factors (CFs) on Incident Costs



The overall costs of an incident are not deterministic. That is, an incident that occurs at one point in time and space may have significantly different costs than an identical one at another point. We believe that an incident has a baseline cost: the most inexpensive way it could be handled appropriately. The model shows that, when specific variables interact with an individual incident and its baseline cost, they have the potential to increase the costs of an incident.

Moreover, we hypothesize that the greater the number of these factors, the greater the potential for higher costs.

After these factors have attached themselves in some sense to a specific incident, we apply our costing methodology, which results in the specific costs of an incident.

These representations of the process for determining the costs of IT incidents should be viewed in their most general sense. We have not determined all factors that impact incident costs. The factors identified are those

that arose from our analysis of the sample of incidents. We believe that the process of developing this model may provide insight into points of intervention for both reducing the occurrence and costs of IT incidents.

According to this model as represented in Figures 1 and 2, reduction in the extent to which factors impinge on baseline potential for occurrence or costs is the point that deserves the most attention.

FINDINGS

We investigated and analyzed 30 IT incidents from the participating universities. At least one incident from each university has been included in the sample. For more specific data about the incidents, refer to Appendixes A and C.

Our findings are presented in three sections. The first explains the cost variables relevant to our discussion. The second presents aggregate data on the overall dollar loss, number of employees involved in each incident, number of hours spent in the resolution, and number of users impacted. The third section provides frequency data for the factors that we identified in the previous section.

Cost Variables

We have identified four categories of incident costs most relevant to the discussion of loss to universities as a result of IT incidents.

1. **Dollars:** Aggregate data on dollar loss from incidents can function as a catalyst for change to existing IT policy. It also is a good benchmark for interpreting the general loss to universities.

2. **Employee time:** An analysis of the employee hours lost (that is, lost productivity) as a result of resolving an incident may signal the need for increased efficiency in incident handling and for recognition of this time as a real loss.

3. **Number of affected users:** This category serves as a proxy for the measure of an incident's impact. Even a small, relatively inexpensive, and short-lived incident may affect many users significantly, resulting in diminished user satisfaction.

4. **Unquantifiable costs:** These are costs which we are unable to quantify explicitly. The unquantifiable costs, however, may prove to be more "costly" than any of the other measures can express. Examples include potential litigation, loss of prestige or reputation, user dissatisfaction, and lowered staff morale.

Aggregate Quantifiable Data

Figure 3 shows the frequency of incidents within a particular range of costs. Note that all data are presented here in terms of the incidents' median costs. When a range of potential costs exists due to user cost estimates, an average was used.

The data show that a majority of the incidents in this sample cost below $50,000. Of those, the greatest number cost between $0 and $15,000. Included in our sample, however, are seven incidents that cost their universities more than $50,000 each.

Figure 3: Total Costs of Incidents

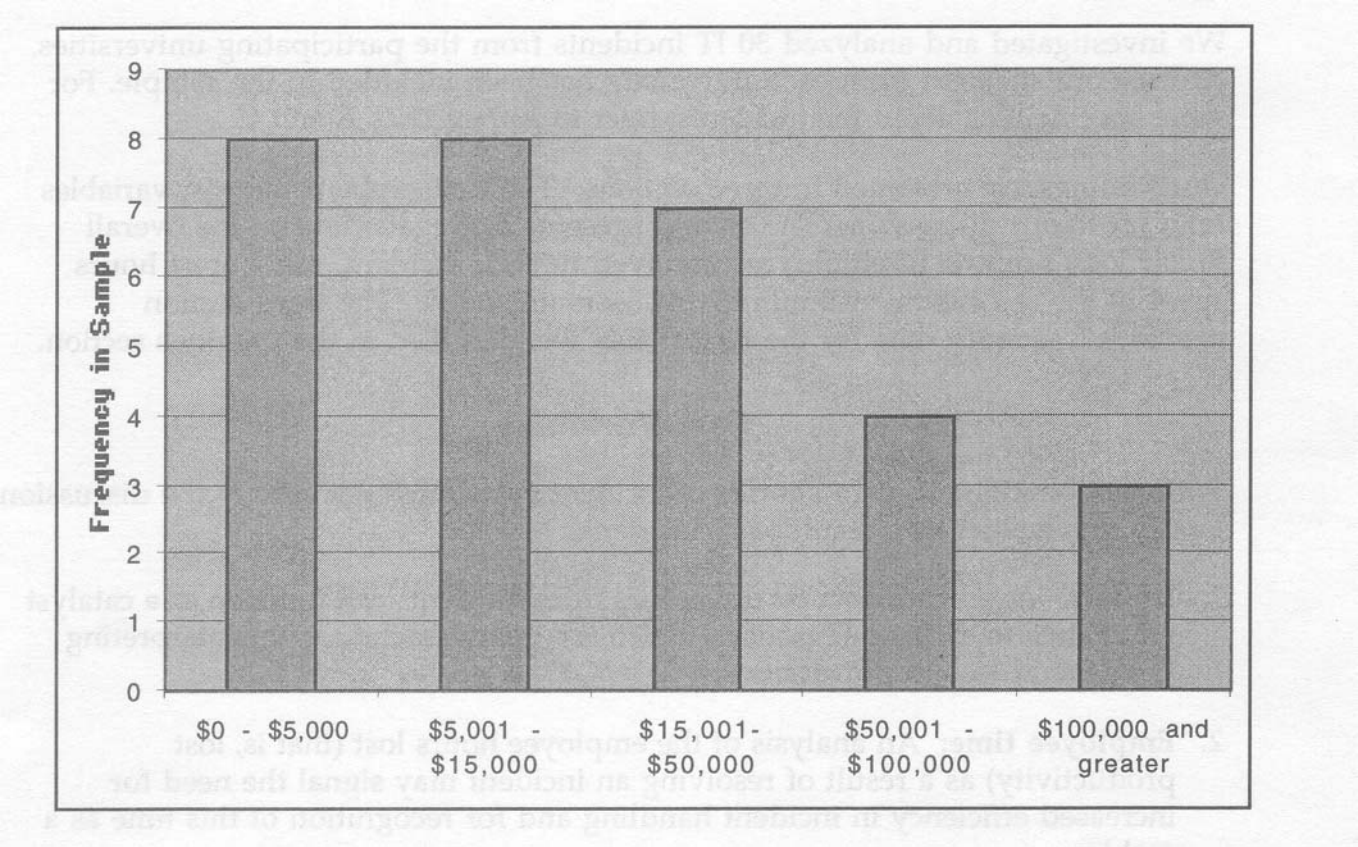


Figure 4 presents the number of employees involved in resolving an incident. The typical incident within our sample had fewer than six employees involved in the resolution, with nearly two-thirds of the incidents involving less than 11 employees. It would be difficult to extrapolate causal relationships in terms of incident specifics because the data is a function of the efficiency and competency of employees, the extent to which an incident becomes public (thus involving public relations employees and often lawyers), and the number of organizational levels of the investigating unit that become involved in resolving the incident.

Figure 4: Number of Employees Involved

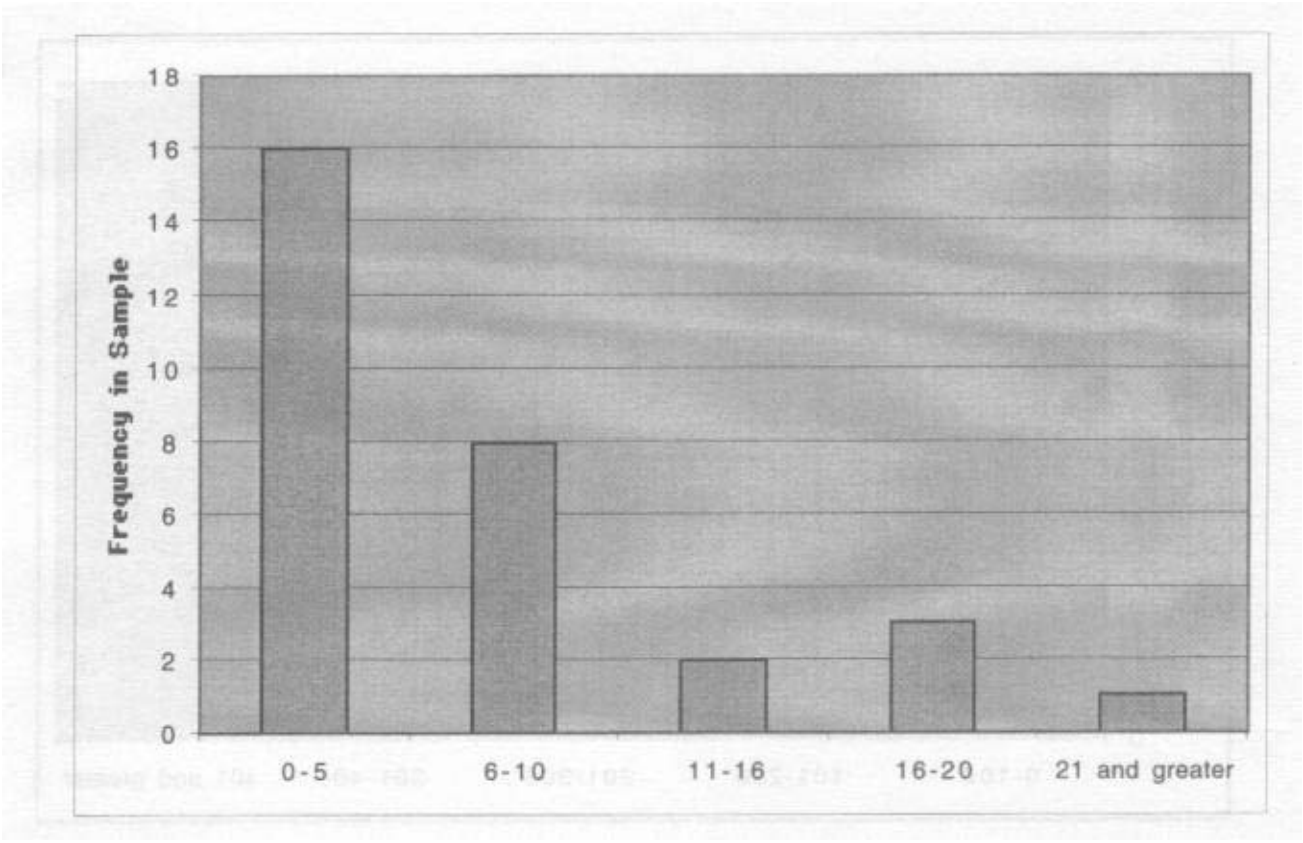


Figure 5 shows the distribution of staff hours needed to resolve an incident. Most of the incidents we investigated and analyzed required fewer than 200 staff hours. This result is not surprising given that most of the incidents in our sample involved fewer than 10 people in the resolution. We would expect that the fewer employees involved, the fewer hours spent resolving the incident.

Figure 5: Employee Hours

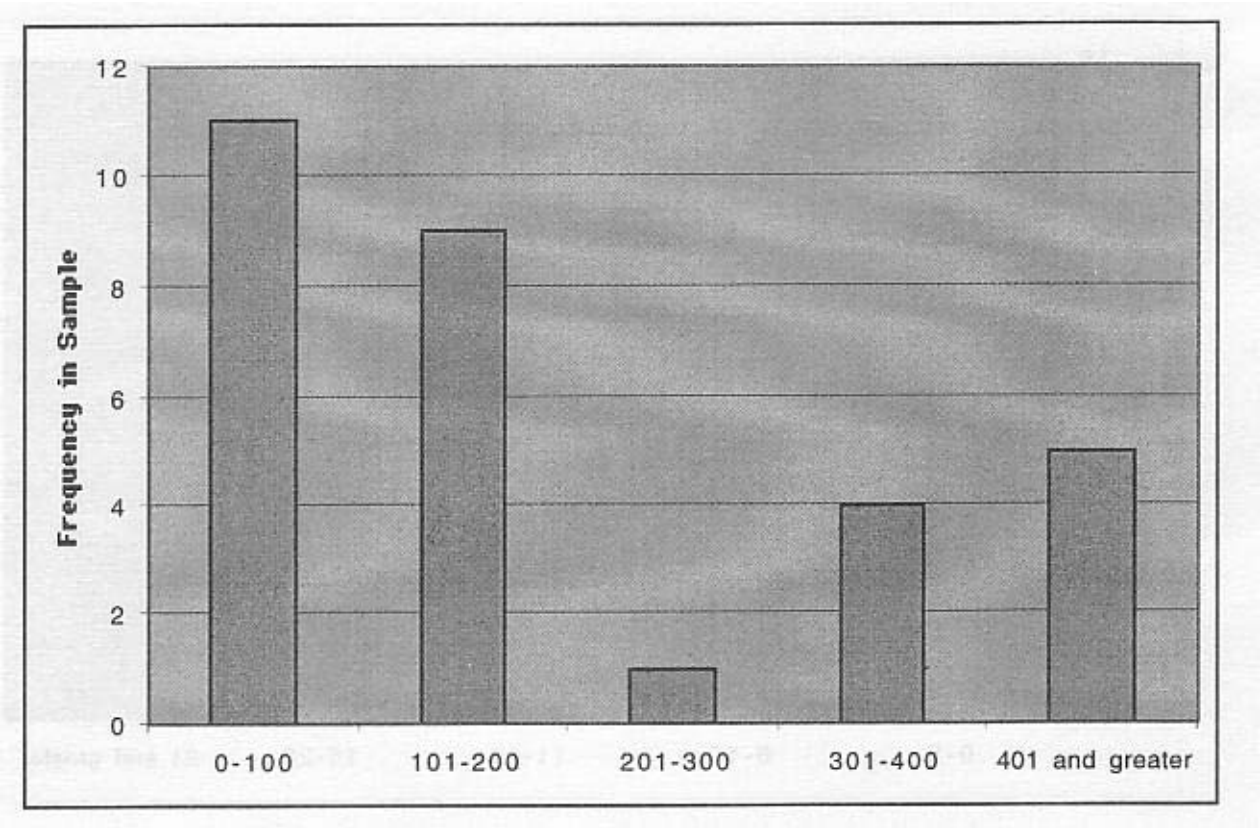
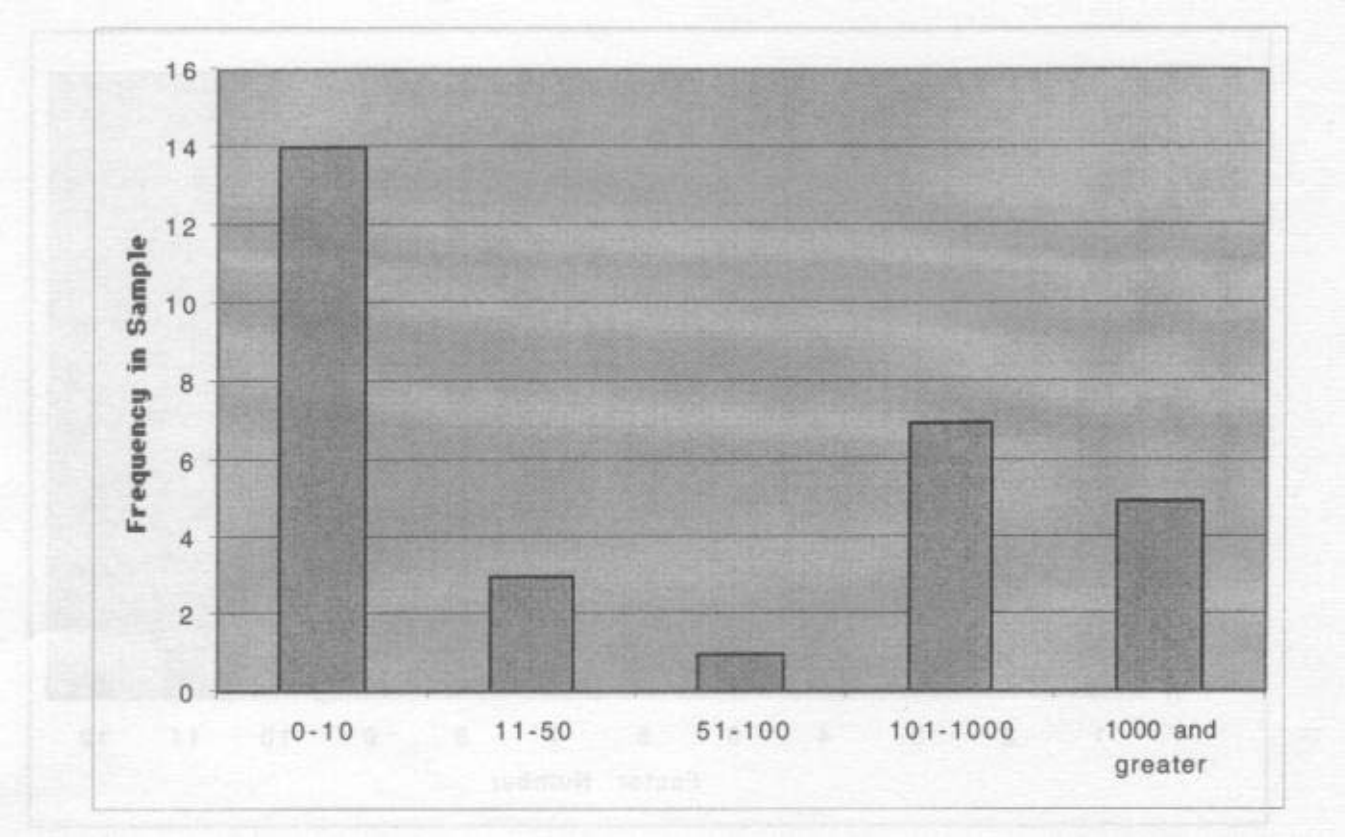


Figure 6 provides aggregate data on the number of affected users. Nearly half the incidents had fewer than ten affected users. Five incidents, however, had 1,000 or more affected users. The number of users affected is generally dependent on the type of incident and the type of service or data that is unavailable. Typically, the most expensive incidents involve large numbers of affected users.

Note that the data presented in Figure 6 often reflect an estimated number of users. The estimate is based on our investigation and conversation with employees involved in the resolution.

Figure 6: Number of Affected Users



Factor Frequency

The following charts provide the frequency data of the factors identified in the model development section. We identified the number of times particular factors were present within our sample and charted them accordingly. Note that the lists of factors are not mutually exclusive, so at times they may overlap. The point of the exercise is to get a better understanding of which factors are most prevalent and, hence, are good areas for security intervention and further study.

Figure 7 shows the number of times a factor influencing the occurrence of an incident was identified in the sample. Refer to Table 1 as a guide for interpreting the chart.

Figure 7: Frequency of Occurrence Factors in Incident Sample

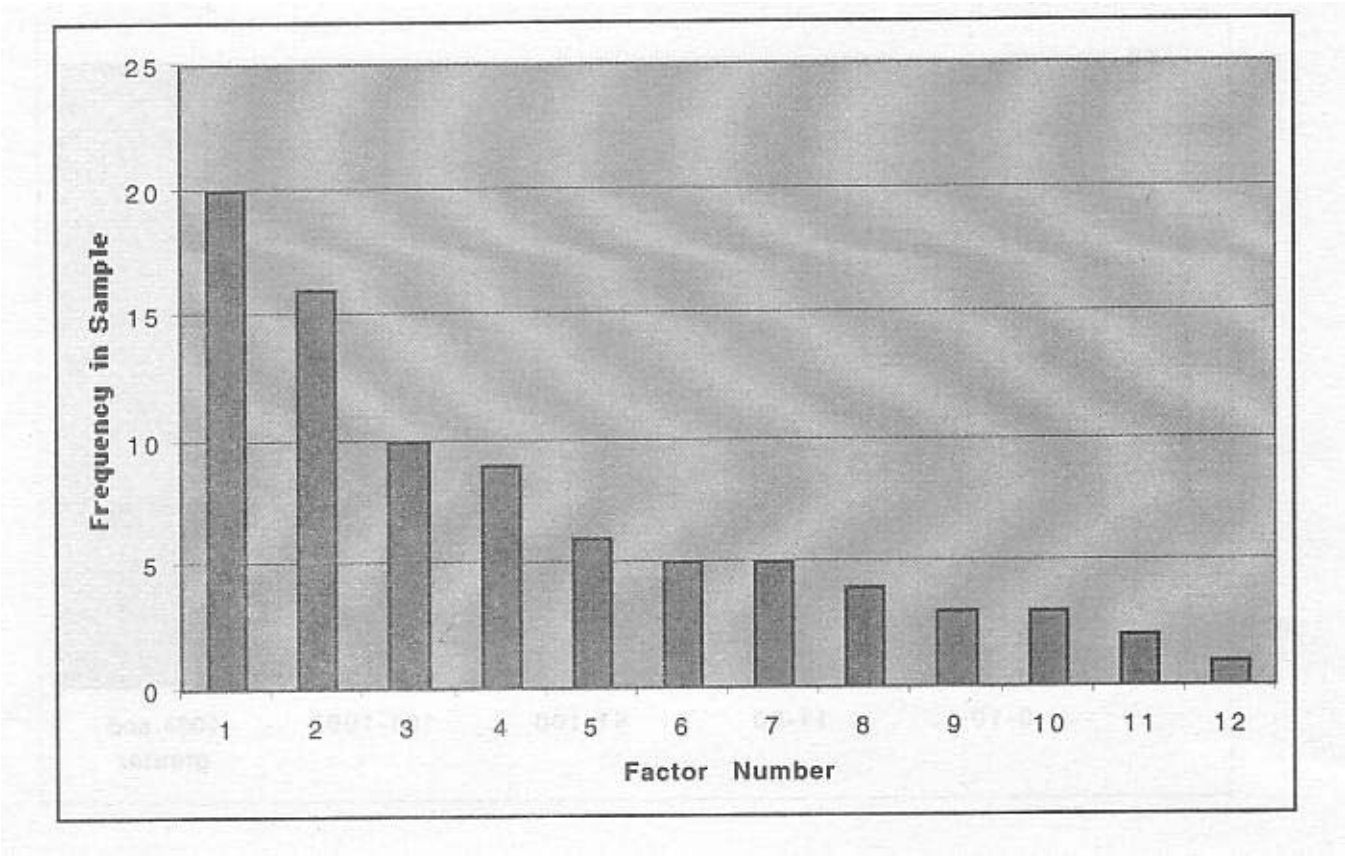


Table 1: Factors with the Potential to Increase Incident Occurrence

1. Openness of System	5. Directions Followed	9. Faulty Equipment
2. Community of Hackers	6. Physical Security	10. Lack of Resources
3. Lack of System Maintenance	7. Appropriate Use	11. Policy
4. Level of Security	8. Training	12. Incompatibility

Our analysis reveals that a hacker community, relative openness of a university system, and lack of system maintenance are the most prevalent occurrence factors. We would expect this result, given the large proportion of hacking incidents relative to the entire sample. The extent to which directions are followed and the appropriate level of security are also relatively prominent. This suggests that better communications between computing personnel and a review of the proper security levels could reduce the occurrence of IT incidents.

Figure 8 indicates the number of times a particular factor with the potential to increase costs was identified. Refer to Table 2 as a guide for interpreting the chart.

Figure 8: Factors Influencing Costs of Incidents

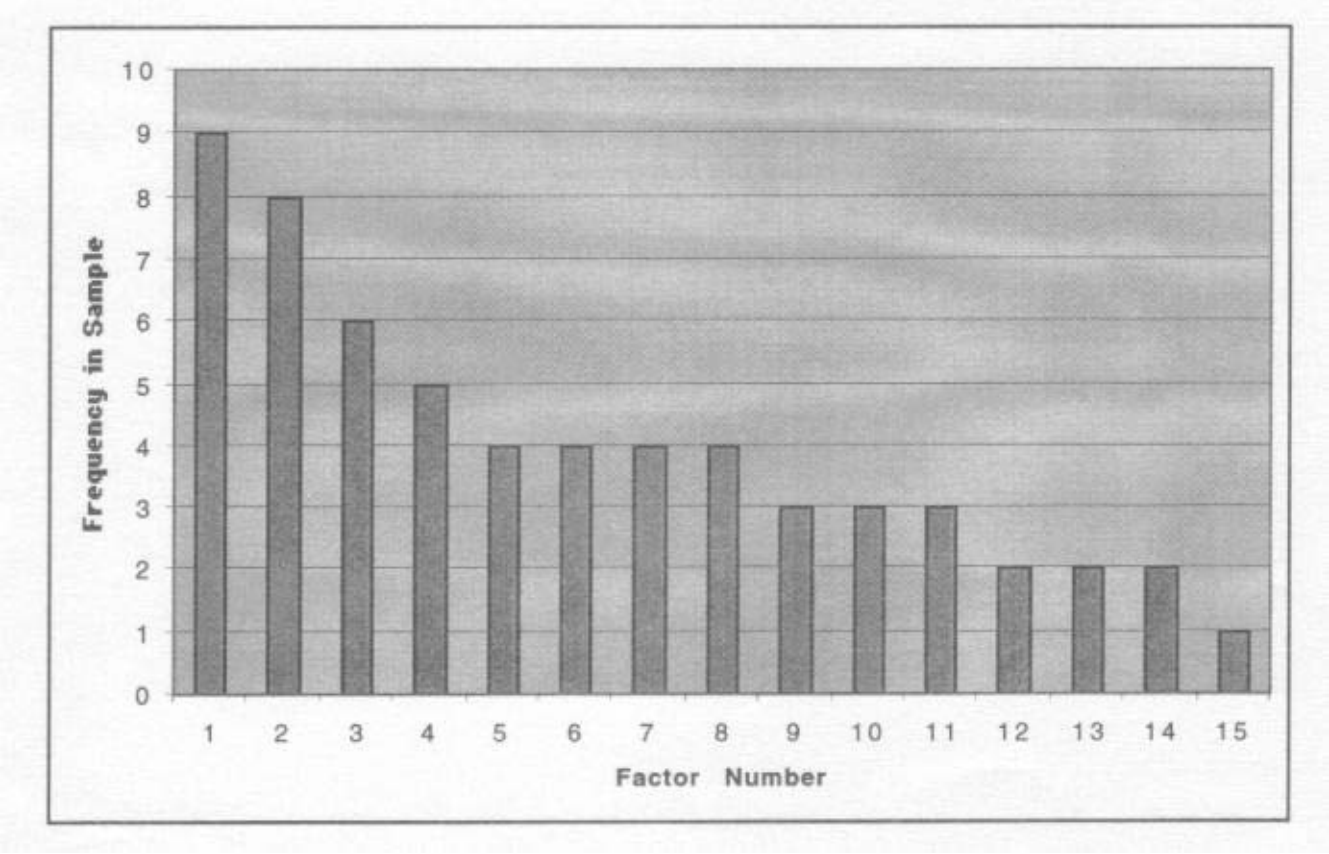


Table 2: Factors with the Potential to Increase Costs

1. Capture vs. Close	6. Complex Configurations	11. Back-up
2. Lack of Knowledge	7. Monitoring Information	12. Age of Systems
3. Coordination	8. Incompatibility	13. Lack of Resources
4. Level of Personnel	9. External Response	14. Timing
5. Loss of Resources	10. Age of Incident	15. Continuity

Our analysis reveals that lack of knowledge, poor incident resolution coordination, and the decision to capture the perpetrator rather than immediately close open holes in hacking incidents are the most prevalent cost factors in our sample. High-level personnel involvement in the sampled incidents is also a common factor. These findings suggest legitimate points of intervention for reducing the potential costs of incidents.

CONCLUSIONS

The intention of the Incident Cost Analysis and Modeling Project is to provide information to technical administrators, managers, and executive officers in order to assist in the implementation and creation of effective IT policy. The methodology developed here is unique because it has begun to identify points of intervention for reducing the potential for the occurrence and costs of IT incidents. The framework developed for understanding the nature of incidents on college campuses has set the foundation for more quantitative research.

Our research has led us to several observations:

- The "capture vs. close" decision is an institutional decision, yet cost tradeoffs accompany the choice. If an institution attempts to identify a hacker, it is implicitly accepting the increased costs due to its investigation and possible legal proceedings. Closing holes, on the other hand, is typically a quick and much less costly fix. The tradeoff lies in the extent to which a successful attempt at catching a hacker deters others from attempting further attacks (which, in the long run, lowers overall costs), and the extent to which simply fixing holes without recourse is an invitation to further attacks.

- We found during this project that many incidents are not well-defined events with a clear beginning and end, but dynamic, on-going interactions. Sometimes an incident does not have a clear ending point due to external and multiple agency involvement. For example, what started out, in one case, as a simple hacker intrusion event led to over eighteen months of investigation, involvement with federal investigators, pending lawsuits, and massive staff time. This issue once again hinges on an institutional "capture vs. close" decision: Is it better to investigate and try to capture an intruder on university systems, thereby deterring other potential penetrations, or better to close holes and cut losses, but possibly perpetuate ongoing attacks?

- Sometimes an incident does not have a clear ending point due to internal deficits and coordination. In one case, for example, lack of system administrator training, the absence of incident handling guidelines, outdated machines, and lack of software resources led to months of system vulnerability and inefficient management of technology, which translates into higher costs. An institutional decision determines this issue as well. How much is it worth to invest in the training of system administrators to meet the complexity of their jobs? How much is it worth to invest in security education for users who contribute to the vulnerability of systems?

- Sometimes an incident is not a singular event, but rather a chain of related misuses or abuses of resources that only later during investigation become connected. We found this to be the case in more than one incident. Unless the connection between these seemingly isolated events becomes evident, resources can be duplicated and wasted and total costs left unidentified. Once again, this issue depends upon an institutional decision. Is it better to manage incidents on a system by system basis within individual units of colleges and universities, or to establish coordinated response procedures that facilitate communication across all units?

- In several incidents that we analyzed, the level of personnel involved in the resolution significantly impacted the overall costs. We found that if an incident garners public attention, vice presidents, lawyers, and public affairs specialists become involved. In many cases, the management hierarchy is such that the delegation of authority must pass through several channels before incident resolution begins. If incident handling could be streamlined to lessen the involvement of upper management, there is the potential for savings.

This study established for the first time an estimate of the actual costs of particular IT incidents. The data as it is presented provides tangible and easily understood costs and figures that may be useful in planning security and security education expenditures.

The ICAMP study has opened channels for sharing information about IT incidents and provided a sample of incident types. Better coordination and communication between and across schools and departments is a necessary step in understanding the types of risks that occur on campuses. Information sharing can be a catalyst for efficiency in proactive protection from IT incidents and swift incident resolution.

The study has provided a template and methodology for IT staff to calculate the costs of incidents on their own campuses. Cost analyses of incidents, once thought to be out of reach, can now be executed quickly and easily at individual campuses.

This project began the identification of factors that appear to affect the occurrence of incidents and those that affect the costs of incidents. The identification of these points of intervention may prove to be useful in reducing the occurrence and costs of future incidents.

Finally, the ICAMP study established a framework and objectives for future study. Much needs to be done before coming to a full understanding of the risks and costs associated with IT incidents. The ICAMP project, however, has established a firm foundation and momentum for future progress.

RECOMMENDATIONS

The ICAMP study has made progress in developing a predictive cost analysis model and understanding the factors that seem to influence IT incidents in university computing environments. However, more needs to be done before specific management recommendations can be formulated. The following are areas for further research.

- **Collect an expanded sample of IT incidents that focuses on selected incident types for cost comparisons across schools.** New incident types should be identified, incidents that arise from or impact the new methods of doing institutional business. An extended sample is required to answer pressing questions that the CIOs and others have: How do the costs of same-type incidents compare when handled at different times of the academic year, within different schools, and by different people? How do the costs of same type incidents compare when the techniques for handling incidents are radically different?

- **Select a sample of individuals-faculty, staff, and students-involved in each particular incident.** Identify incidents that affected a community of users, such as server crashes or disabled networks. Calculate full costs for the entire population that experienced the incident through extensive interviews of each sample to determine the actual costs incurred by these individuals due to revised work routines, delayed production, and opportunity costs.

- **Collect frequency data on selected incident types to further our understanding of the effects of IT incidents.** This data will allow universities to estimate overall losses over a specific time period. The collection of frequency data is also necessary to complete the work on a predictive cost analysis model.

- **Measure the relative strengths of the factors identified in this project on cost variables.** Quantification of the effects of the identified factors that influence the occurrence and costs of incidents may shed more light on security education and preventive measures to be taken.

- **Measure the difference in data collected while an incident is occurring through to its resolution and the data collected three to six months following the incident**. Determine whether the resources involved in managing the incident appear significantly less in retrospect than the actual costs.

The CIOs initially funded ICAMP to provide the beginnings of a predictive cost model and to analyze the costs of a sample of incidents. We now need to move from an understanding of the sample of IT incidents and their costs to recommended solutions. Through an expanded sample, comparisons of incidents of the same type, information about frequencies, and an expansion of factor analysis, the project can provide more specific recommendations to managers. Does the incident sample reveal obvious policy gaps? Are there obvious tool or skill gaps? Does the sample reveal best management practices that are going unheeded? Do information security procedures need to be put in place? Recommendations need to be made, in conjunction with members of the CIC Security Working Group, for actions that managers and others should take to reduce, eliminate, or manage the IT risks that have been identified.

Appendix A
TYPES OF IT INCIDENTS

The following describes the types of incidents that we have investigated and analyzed. The categorization here is for clarity and an understanding of the breadth of our sample only.

- **Hacker incidents:** A large percentage of our incident sample falls into the hacking category. These incidents involve unauthenticated access to university systems, both internal and external. At times the hacker was simply trying to gain access to a system. Other times the intent was malicious.

- **Theft incidents:** Our sample includes hardware and software theft as well as information theft.

- **Infrastructure failure:** These incidents cause complete systems to shut down because of a loss of power or other physical processes. Difficulty in measuring user loss as a result of this type of incident makes them one of the more troublesome to quantify.

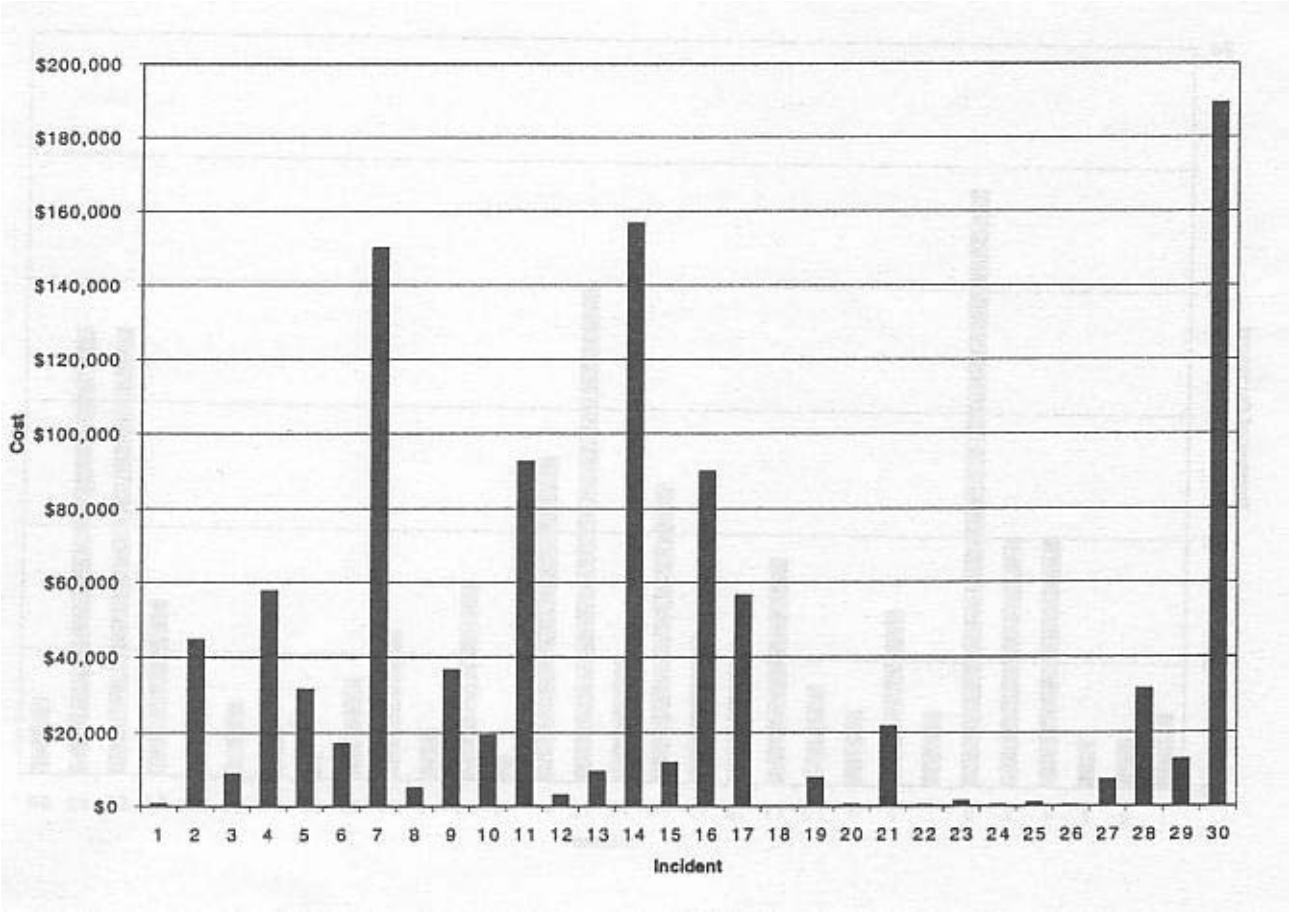
- **Denial of service:** These incidents are malicious attacks that prevent users from accessing information technology resources.

- **Nonmalicious data loss:** This category is meant to distinguish itself from others by intent. The incidents in this category are often a result of lack of policy, procedure, or knowledge of a system.

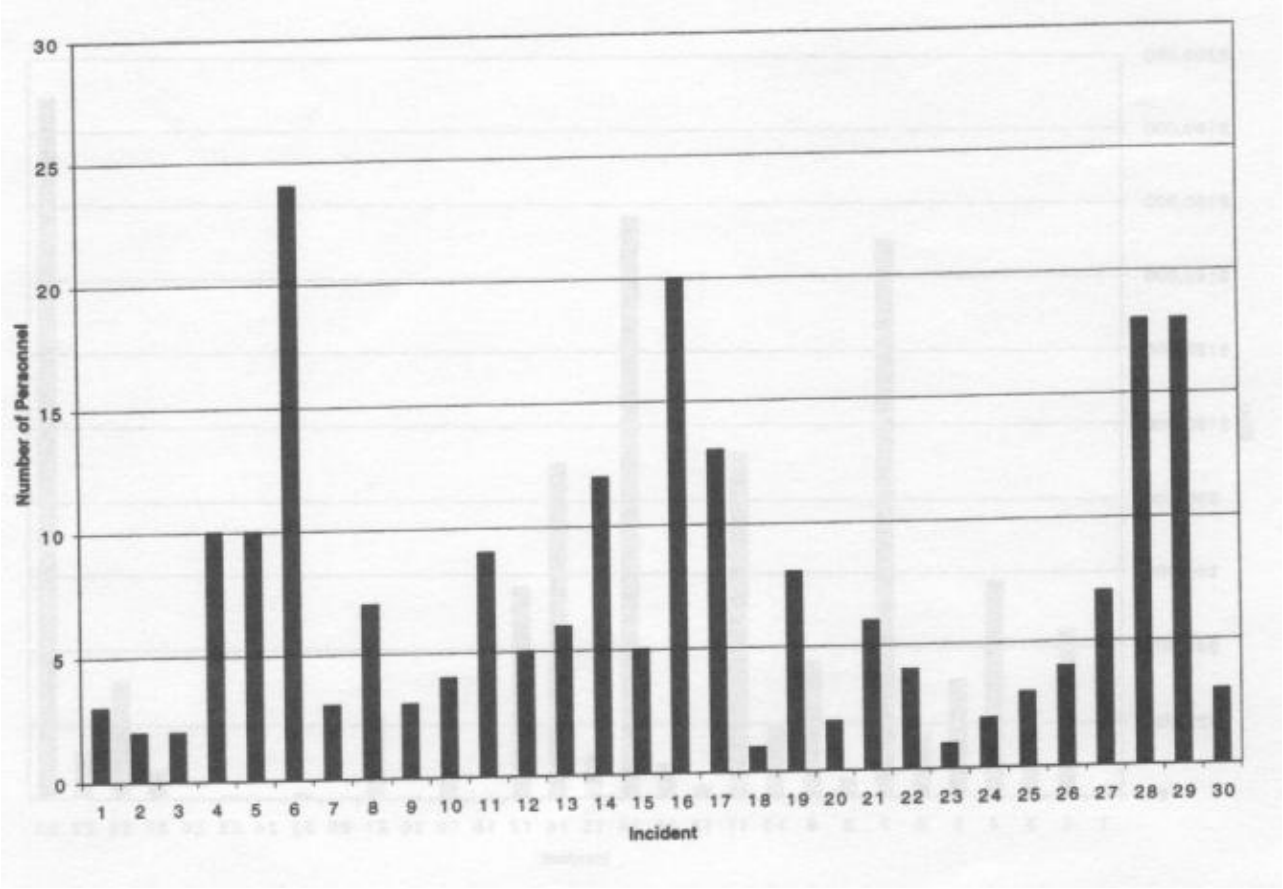
Incident Specific Data

	Incident	# of Emp. Hrs.	# of Personnel	# of Users	Total Cost	Error Bound (+/-)
1	Bomb Squad	14	3	1	$600	$100
2	Downtime on the Web	91	2	350	$44,450	$22,250
3	Dropped Egg	122	2	135	$8,600	$1,300
4	Exposed SSN	304	10	1,100	$57,500	$8,100
5	Give Inch/Take Mile	355	10	25	$31,400	$4,800
6	Horse in Public Site	407	24	75	$17,000	$4,150
7	Infamous Hacker Gang	3790	3	0	$150,000	$18,900
8	Interrupted UPS	107	7	80,000	$4,700	$700
9	Invasion - Body Swappers	118	3	0	$36,400	$800
10	Juvenile Delinquent	320	4	10	$19,100	$2,900
11	LAN Crash	288	9	0	$92,500	$13,800
12	Linux Crack	59	5	12	$2,900	$400
13	Mismanaged Machine	190	6	150	$9,300	$1,400
14	Missing Donors	194	12	180,000	$156,500	$21,200
15	Missing Multimedia	173	5	0	$11,700	$400
16	Night the Lights Went Out	31	20	4,500	$90,000	$30,000
17	Overflowing Buffer	551	13	2,500	$56,300	$8,400
18	Phony FBI Agent	1	1	1	$30	$5
19	Politics/Gopher	190	8	15	$7,600	$1,100
20	Posted Passwords	5	2	5	$210	$30
21	Spawning	377	6	1,000	$21,400	$2,800
22	StatD Overflow	2	4	0	$100	$20
23	Stolen Identity	20	1	1	$1,200	$200
24	Student Threatened to Death	3	2	0	$150	$20
25	Swedish Bouncer	16	3	0	$700	$100
26	Swiped Card	4	4	0	$120	$20
27	Telnet Demon	178	7	24	$7,100	$1,100
28	Unauthenticated Satellite	621	18	900	$31,400	$4,400
29	Unidentified Hacker	464	18	0	$12,600	$1,900
30	Upgrade Disaster	188	3	352	$189,300	$70,000
	TOTAL	9,078	210	270,805	$1,015,810	$198,945

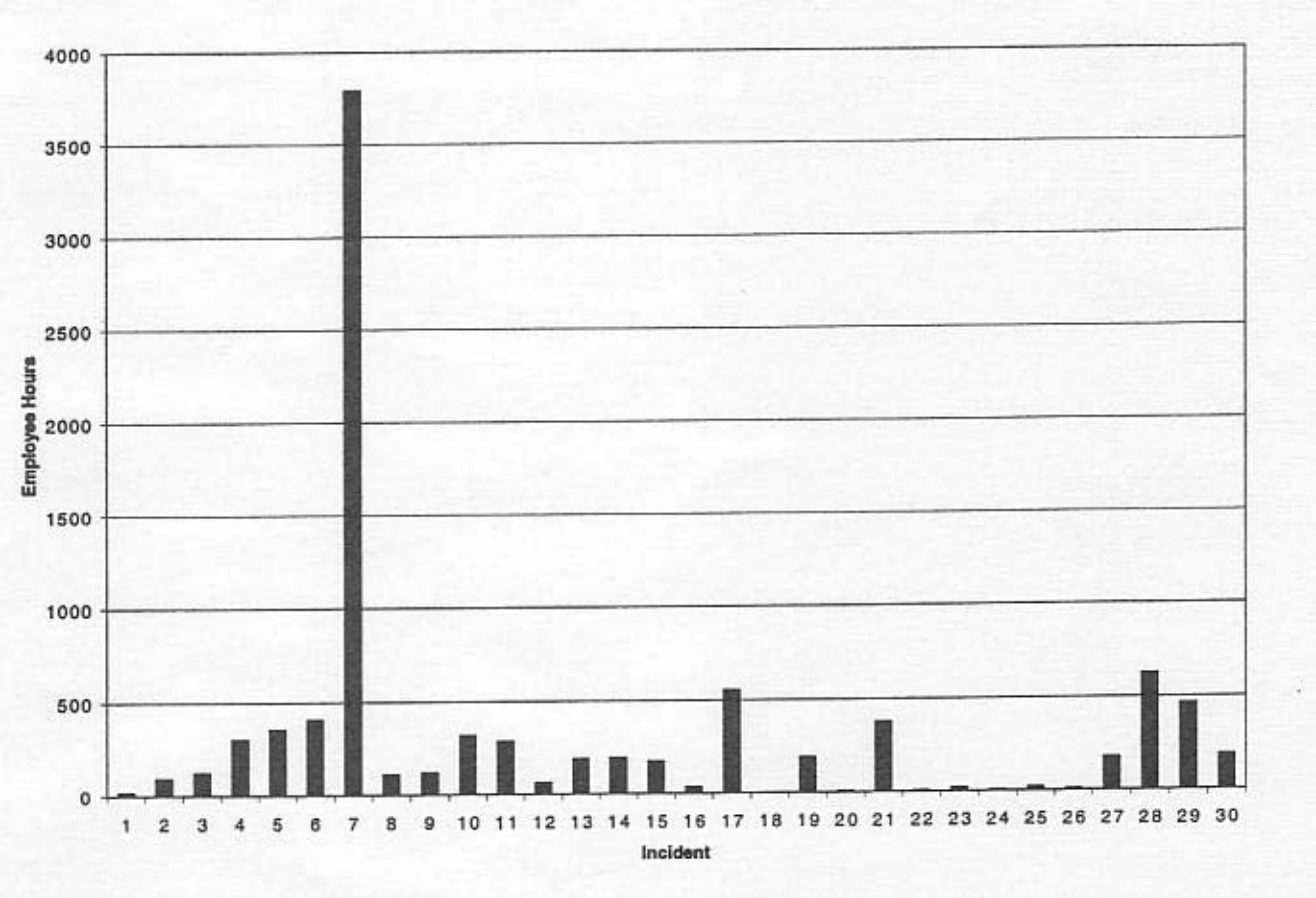
Total Costs


$200,000
$180,000
$160,000
$140,000
$120,000
$100,000
$80,000
$60,000
$40,000
$20,000
$0
Cost
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Incident

Number of Personnel



Employee Hours



Appendix B
CONVENTIONS FOR COST VARIABLES

This appendix provides information about the way the study treats specific cost variables.

Costs on the Resolution Side of the Incident

This factor refers to the wage costs attributable to the efforts of faculty, staff, students, and consultants responsible for resolving an incident.

Faculty, Staff, and Student Employees

To account for the costs of employees in resolving incidents, we have followed a conservative convention. With deference to the possibility of error in recalling past events and protecting ourselves from reporting data with a false sense of precision, we calculate wage costs within a confidence interval of 15%. We cannot be certain of the appropriate level of confidence to use, but feel that +/- 15% is a fairly large error bound and, if anything, errs on the side of slightly underestimating costs. It is, however, a necessary procedure given the uncertainty in data collection.

The actual calculation consists of dividing an individual's wage rate by 52 weeks per year and 40 hours per week to obtain an hourly wage. The wage rate is then multiplied by the reported logged hours, varied by +/- 15% of the reported total, and an interval and median identified. This median figure is used in the total cost figures. Our calculations are explicit in each incident summary report.

Consultants

Incident resolution often requires the assistance of a technical consultant. If the consultant is not part of the particular university, we used the fee charged as the real cost. If the consultant is part of the university-for example, from an information technology center-his or her real wage rate is considered a cost to the university, even if a department pays a consulting fee above that wage rate to the center.

Benefits

Benefits are included in faculty and staff costs where appropriate. We use 28% as a standardized benefits rate. This is a representative measure for the benefits rates of each institution included in the study.

Costs on the User Side of the Incident

During the investigation and analysis of an incident, user costs are consistently the most difficult to estimate. User costs consist of costs borne by the clients of a system, network, PC, and so on, due to malfunctioning equipment, lost data, disclosure of sensitive information, or denial of service. Any time a user is unable to use a system that he or she desires to access or must restore lost data, a cost is associated with the wasted time.

The difficulty in estimating the costs to users is threefold. First, it is virtually impossible to speak to every affected user to determine his or her real loss in dollars. Second, we cannot say for certain what the user's time is worth. Wage rates are traditional measures of a person's time, but it is difficult to put a number on, for instance, a student who is not employed. Third, opportunity costs are always involved. If a person cannot retrieve needed information from the network, he or she may be able to do some alternative activity that

provides some utility. Measuring the difference between the real loss and gain in utility from an alternative activity is a difficult task at best.

When we encountered situations that involved estimating the costs to users, we provided reasonable scenarios for overall costs based on the data we gathered during the incident investigation.

Other Cost Factors

Indirect Cost Rates

Indirect cost rates (ICR) are included in faculty and staff costs where appropriate. We use 52 percent as a standardized ICR. This is a representative measure for the benefits rates of each institution included in the study.

New Purchases

If hardware or software purchases are required to return a system to its original state, the purchase price has been included as a cost of the incident. However, if the purchase of new equipment is only expedited by an incident, meaning the purchase was inevitable but not planned for at that time, then we have not included it as part of the incident's cost. (Refer to "Methodology, Assumption 4" for an explanation.)

Investigation Template

I. NAME OF THE INCIDENT:_____

- You should provide a non-identifying name to use for future reference.

II. DETAILED DESCRIPTION OF THE INCIDENT:

- Incident Type:
  - ❑ Disk or server crash
  - ❑ Virus
  - ❑ Hardware/ Software Theft
  - ❑ Hacker activity (will include sniffers, Trojan Horse etc.)
  - ❑ Other _____
- Duration of the Incident:
  - ❑ Less than one week
  - ❑ 1 -2 weeks
  - ❑ 2 weeks - one month
  - ❑ 1 -6 months
  - ❑ more than 6 months
- Level of incident:
  - ❑ Restricted to individual
  - ❑ Restricted to department
  - ❑ Restricted to College (Dean Involvement)
  - ❑ University level involvement (Executive Officers, Public Relations)
  - ❑ Multi-institutional involvement
  - ❑ Other

- University or Campus Police involvement?
  - ❑ Yes
  - ❑ No
- Written Description (feel free to add additional pages as needed):

III. CHRONOLOGICAL DESCRIPTION OF THE RESOLUTION:

- The order of the steps used in correcting the problem may matter depending on how we choose to close out the quantification of the incident.

- Describe the steps taken and their approximate dates.

IV. PEOPLE INVOLVED IN THE RESOLUTION:

- Please provide an exhaustive list of the names, telephone numbers and email addresses of the people involved in the incident's resolution.

Name	Logged Hrs.	Phone #	Email	Salary

V. IMPLICATIONS FOR USERS:

- What are the ramifications of the incident?

- Who did the incident affect and how?

- Approximately how many users were affected?

- Were these users faculty, staff, students, or a combination of the three? (If combination, please provide an estimate of the percentage of the type of user – for example : 45% faculty, 55% staff)

- What is the average wage for these users:
  - ❑ Faculty _____
  - ❑ Staff _____
  - ❑ Graduate Students _____
  - ❑ Undergraduate Students _____

VI. NEW PURCHASES:

VI. NEW PURCHASES:

- Were you required to purchase new hardware, software and the like to return your system to its original state?

  ❑ Yes

  ❑ No

- If yes, what type of equipment was purchased and what was its cost?

Equipment	Cost of Equipment

VII. CONSEQUENCES:

- What has happened as a result of the incident?

- Are there more reported incidents of the same type?

- Have new positions been created?

- Is the network or office managed differently?_____

VIII. PREVENTION:

- What could have reduced costs?_____

IX: SAMPLE SPREADSHEET:

Workers Costs					
Title	Logged Hours	Hourly Wage	Total	-15%	15%
Subtotal					
Benefits @28%					
Subtotal (Staff Salaries + Benefits)					
Lab Assistants					
Indirect Cost Rate					
Total Labor Costs					
Median Estimates					
User Costs					
Number of Users	Total Estimated Hours	Value of Time	Total	-15%	+0.15
Median Estimate					
Total Costs					
Workers Costs					
User Costs					
TOTAL COSTS					

Appendix C
INCIDENT REPORTS

Appendix C consists of all ICAMP incident reports, numbered to match the tables found in Appendix A. Each report begins with a description of the incident and its resolution and concludes with a discussion of the costs and incident implications, including spreadsheets which detail all findings.

Please refer to Appendix B for methodology and cost conventions.

All identifying information about each institution has been removed from the reports to preserve anonymity.

1. The Bomb Squad

The Incident and Its Resolution

During the fall of 1997, a student reported to campus police and the campus dean that she received over 720 harassing e-mail messages in a short period of time. The mail bomb had the effect of denying the student access to her e-mail account for approximately one full working day.

The university's computing incident investigator was contacted to ascertain the origin of the e-mail. A search through various connection logs revealed that the messages were sent from a small non-CIC institution. The incident investigator requested that an inquiry into the incident be handled locally by the other school's investigating unit.

The non-CIC institution identified the individual responsible for the harassing messages and confronted the student. The student claimed that an individual at the CIC institution requested that he send the messages to the victim from his computing account. The incident investigator believes that the two students conspired to execute the mail bomb in this manner because 1) they wanted to protect the identity of the CIC institution student, and 2) the CIC institution student didn't have the appropriate resources to carry out the mail bomb easily.

Approximately two days after the original complaint, the CIC institution student was confronted by campus police about the harassing messages. The student admitted to asking the other individual to send the messages and was subsequently issued a disorderly conduct ticket by campus police. The student was also referred to the Dean of Students office for disciplinary action.

To clean up the victim's account, the incident investigator deleted the messages, taking care to not destroy legitimate mail.

Costs and Incident Implications

Our calculations reveal a total quantifiable cost to the university of **$600**. This figure includes the wage costs attributable to resolving the incident and the costs accrued during the period in which the victim was unable to access her e-mail account.

Cooperation between the two schools significantly reduced the investigation time and brought about a swift resolution to the incident. The individual responsible for the attack was expelled from the CIC institution.

Although the event was fairly traumatic for the victim, little could have been done to prevent the incident. The victim did the correct thing in contacting the Dean of Students office and the campus police.

Workers' Costs

Three university employees were involved in resolving the incident for a reported 14 hours. The incident investigator's time was spent tracking the origin of the message, coordinating the work between the two schools, and writing reports. An individual from the Dean's office interviewed the victim after the initial complaint, and a campus police officer interviewed the CIC institution student and detailed the incident in various reports.

Using reported logged hours and wage rates, we estimate that the total cost attributable to the individuals involved in resolving the incident was $600. This figure does not include any time spent by individuals at the non-CIC institution (see Table C-1).

Table C-1

Workers' Cost					
Title	Hours	Hourly Wage	Total	-15%	15%
Incident Investigator	6	$16.31	$97.85	$83.17	$112.53
Disciplinary Officer	2	$41.47	$82.94	$70.50	$95.38
Campus Police	6	$19.38	$116.28	$98.84	$133.72
Subtotal	14		$297.07	$252.51	$341.63
Benefits			$83.18	$70.70	$95.66
Subtotal (Salaries + Benefits)			$380.25	$323.21	$437.28
Indirect Costs			$197.73	$168.07	$227.39
Total Labor Costs			$577.97	$491.28	$664.67
Median Costs +/- 15%				$577.97	+/- $86.70

Users' Costs

The student victim was without an e-mail account for approximately one full working day. To account for this lost time, we estimated that an average student's wage rate is $6.00 per hour and created a number of productivity loss scenarios based on that assumption. Given that the e-mail account was unavailable for one full working day, we can assume that the student lost between zero and eight hours of productive time. See Table C-2 for details.

Table C-2

Users' Costs			
Number of Users	Hours	Cost/Hr	Total
1	0	$6.00	$0.00
1	1	$6.00	$6.00
1	2	$6.00	$12.00
1	4	$6.00	$24.00
1	8	$6.00	$48.00
Total Costs		$0.00 - $48.00	

Given the non-critical nature of e-mail, however, we would estimate that the overall productivity loss to the student was very low. We estimate that total loss to the student was well under one hour.

Total Cost

The total quantifiable costs of the incident are shown in Table C-3.

Table C-3

Total Costs				
Workers' Costs			$577.97	+/- $86.70
Users' Costs			$0.00	- $48.00
TOTAL COSTS			$577.97	+/- $134.70
Rounded to Nearest $100			$600	+/- $100

Unquantifiable Issues

Personal safety was a concern for the victim because of the nature of the harassing messages. Although we cannot quantify the psychological trauma of the event, it should be considered a real cost of the incident.

The mail bomb temporarily denied the victim access to e-mail. Other than the productivity loss we tried to capture above, this delay may have caused the victim to miss important messages for school or work. This inconvenience should be considered a real cost attributable to the incident.

2. Downtime on the Web

The Incident and Its Resolution

A system administrator contacted a technology specialist at his university stating that it appeared someone had hacked into his school's Web server. He determined that it was probably a hacker because the root password was changed and logs had been deleted. Only one UNIX machine was compromised and little, if any, alteration or destruction was noted.

The technologist gave the system administrator all needed patches and the system administrator began to secure the server. To correct the UNIX machine, it had to be down for three working days. Although no new problems have arisen, the system administrator still has, and probably will continue to have, residual problems.

Costs and Incident Implications

The total cost of this incident is potentially between **$22,200** and **$66,700**. This range is a result of the indeterminable nature of the users' costs, which will be discussed at length in the section titled "Users' Costs."

Workers' Costs

Two employees reported a total of 91 hours spent investigating and resolving the incident at a total cost of $3,100. Details can be found in Table C-4.

Table C-4

Workers' Costs					
Title	**Hours**	**Cost/Hr.**	**Total**	**-15%**	**15%**
System Admin	80	$18.00	$1,440.00	$1,224.00	$1,656.00
Technologist	11	$16.11	$177.21	$150.63	$203.79
Subtotal	91		$1,617.21	$1,374.63	$1,859.79
Benefits @28%			$452.82	$384.90	$520.74
Subtotal (Salaries + Benefits)			$2,070.03	$1,759.52	$2,380.53
Indirect Costs			$1,076.41	$914.95	$1,237.88
Total Labor Costs			**$3,146.44**	**$2,674.48**	**$3,618.41**
Median Costs +/- 15%				**$3,146.44**	**+/- $471.97**

Users' Costs

As stated above, the Web server was not available to users for a total of three days. Therefore, users of the server could not use any Web services offered by the school. This could have affected school projects, course materials, or personal Web use.

It was impossible for us to determine how much time each user uses the server in an average day, but we were able to make an estimate based on the information we received.

Of the 250 users who used the compromised server, approximately 200 were graduate students; the other 50 were faculty members. We first determined the potential user costs for graduate students, which can be found in Table C-5.

Table C-5

Individual Users - Grad Students						
Potential Users	Hours	Salary	Subtotal	Benefits	Indirect Cost	Total
200	0	$12.00	$0.00	$0.00	$0.00	$0.00
200	4	$12.00	$9,600.00	$2,688.00	$1,397.76	$13,685.76
200	8	$12.00	$19,200.00	$5,376.00	$2,795.52	$27,371.52
200	12	$12.00	$28,800.00	$8,064.00	$4,193.28	$41,057.28
200	16	$12.00	$38,400.00	$10,752.00	$5,591.04	$54,743.04
200	20	$12.00	$48,000.00	$13,440.00	$6,988.80	$68,428.80
200	24	$12.00	$57,600.00	$16,128.00	$8,386.56	$82,114.56

For the purpose of this analysis, a day equals eight working hours. Although a student's day may be longer or shorter than eight hours, it seemed reasonable for the purposes of this study to equate a student's day with a regular working day.

We used the common wage rate of $12 an hour for all graduate students and varied the extent to which the users may have been affected. It is unclear how much each user was affected, but we can assume that it was somewhere between no time loss and three working days, or 24 hours.

Fifty faculty members were also affected as a result of the server downtime. We used an average wage rate of $30 an hour and, as in Table C-5, varied the extent to which the users may have been affected. Please refer to Table C-6 for details.

Table C-6

Individual Users - Faculty						
Potential Users	Hours	Salary	Subtotal	Benefits	Indirect Cost	Total
50	0	$30.00	$0.00	$0.00	$0.00	$0.00
50	4	$30.00	$6,000.00	$1,680.00	$873.60	$8,553.60
50	8	$30.00	$12,000.00	$3,360.00	$1,747.20	$17,107.20
50	12	$30.00	$18,000.00	$5,040.00	$2,620.80	$25,660.80
50	16	$30.00	$24,000.00	$6,720.00	$3,494.40	$34,214.40
50	20	$30.00	$30,000.00	$8,400.00	$4,368.00	$42,768.00
50	24	$30.00	$36,000.00	$10,080.00	$5,241.60	$51,321.60

We estimate that users lost somewhere between 4 and 12 hours of productivity as a result of the downtime. The Web server is used heavily at this particular school. However, at the time of the intrusion, classes were just beginning a new semester. Thus, new students did not have any documents stored on the Web servers. The

faculty members and the students who were taking classes before the semester, however, were probably more affected, especially those faculty members who had class materials stored on the server and needed them for the first few days of classes. Therefore, we estimated that an average user lost between 4 and 12 hours of working time as a result.

Approximately 100 additional users were affected by the downtime. These users were organizations or staff groups that had materials stored on the server. We were unable to quantify the cost of this lost time because it was impossible to determine whether those users were faculty, staff, or students. Consequently, we were unable to determine a reasonable wage for these individuals. However, these were real costs that should be included in the total cost of the incident.

The total quantifiable user costs are detailed in Table C-7.

Table C-7

Total User Costs - Students and Faculty	
Total Student Costs	$13,685.76 - $41,057.28
Total Faculty Costs	$8,553.60 - $25,660.80
Total User Costs	**$22,239.36 - $66,718.08**

Total Costs

The total quantifiable monetary cost of the incident was calculated by adding the workers' and users' costs. However, given the relative insignificance of the workers' costs (in terms of overall dollar loss), and to guard against a false precision, we did not explicitly include the $3,100 in workers' costs in the total. They should, however, be considered real in terms of the overall incident. See Table C-8 for details.

Table C-8

Total Costs		
Workers' Costs	$3,146.44	+/- $471.97
Users' Costs	$22,239.36 - $66,718.08	
TOTAL COSTS	**$22,239.36 - $66,718.08**	
Rounded to Nearest $100.00	**$22,200.00 - $66,700.00**	

Unquantifiable Costs

We were unable to quantify the group user costs in relation to the downtime of the server for reasons stated in "Users" Costs"' above. However, these are real costs that have the potential to increase the range of total costs.

3. The Dropped Egg

The Incident and Its Resolution

A network services manager found several IRC servers, including one called "Eggdrop," running from a departmental mail server. The unknown person who installed these programs had accessed several accounts, probably through a sniffer, and had stolen the password file from the server.

Initially, the department did not want to investigate. Later, they decided that they did wish to identify and prosecute the individual. This delayed decision made it very difficult to trace the individual and left the senior computing specialist with few options on how to proceed.

The computing specialist traced the activity back to three sites. One site did not respond to requests for help in identifying the individual. With assistance from the other two sites, however, the computer specialist was able to identify the perpetrators as high school students.

At this point the activity seemed to have stopped. There were still additional problems because the department did not follow through with recommended procedures for cleaning up the incident. Rather than request that all users on the server change their passwords immediately to ensure that any additional break-ins would be difficult, the department decided to address the owners of the compromised accounts one by one. Approximately 200 users were identified and asked to change their passwords. Many of these users did not change passwords at first because they misunderstood the instructions and thought their passwords were "safe." Therefore, the network service manager had to deal with these individuals twice.

According to the computing specialist, all investigation stopped at this point. The computing specialist assumed that appropriate measures were taken to close the holes. However, at least one other similar incident occurred after this incident, but it may have been continuing activity from this one.

Costs and Incident Implications

This incident cost the university an estimated **$8,600**. This figure represents a total of the workers' costs and the users' costs in time spent changing passwords.

Workers' Cost

Two employees spent 122 hours resolving this incident. Workers' costs were calculated using real wage data and reported logged hours. See Table C-9 for details.

Table C-9

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Sr. Comp. Specialist	90.0	$31.25	$2,812.50	$2,390.63	$3,234.38
Sr. Mgr. Network Svcs.	32.0	$19.71	$630.72	$536.11	$725.33
Subtotal:	122.0		$3,443.22	$2,926.74	$3,959.70
Benefits @ 28%:			$964.10	$819.49	$1,108.72
Subtotal (Salaries + Benefits):			$4,407.32	$3,746.22	$5,068.42
Indirect Cost Rate (52%):			$2,291.81	$1,948.04	$2,635.58
Total Labor Cost:			**$6,699.13**	**$5,694.26**	**$7,704.00**
Median Cost +/- 15%			**$6,699.13**	**+/- $1,004.87**	

Users' Costs

Many students, faculty, and staff members had to change their passwords as a result of this incident. We calculated the students' user costs without including benefits or indirect cost rates because they are not employees of the university.

Users' costs for the faculty and staff members included these rates. We added the subtotals for the three user groups to get a total user cost for this incident. See

Table C-10 for more information.

Table C-10

Users' Costs					
Number of Students	# of Hrs.	Cost/Hr	Total	-15%	15%
80	40	$12.00	$480.00	$408.00	$552.00
Subtotal	40		$480.00	$408.00	$552.00
Number of Staff	# of Hrs.	Cost/Hr	Total	-15%	15%
10	5	$12.01	$60.05	$51.04	$69.06
Number of Faculty	# of Hrs.	Cost/Hr	Total	-15%	15%
45	22.5	$28.85	$649.13	$551.76	$746.49
Subtotal:	27.5		$709.18	$602.80	$815.55
Benefits @ 28%:			$198.57	$168.78	$228.35
Subtotal:	67.5		$907.74	$771.58	$1,043.91
Indirect Cost Rate (52%):			$472.03	$401.22	$542.83
Total Staff & Faculty Costs:			$1,379.77	$1,172.81	$1,586.74
Total Student Costs			$480.00	$408.00	$552.00
Total Users' Costs:			**$1,859.77**	**$1,580.81**	**$2,138.74**
Median Cost +/- 15%			$1,859.77	+/- $278.97	

Total Costs

The total costs to the university for this incident were determined by adding the workers' and users' costs. See Table C-11 for details.

Table C-11

Total Costs				
Workers' Cost			$6,699.13	+/- $1,004.87
Users' Costs			$1,859.77	+/- $278.97
Total Costs			**$8,558.90**	**+/- $1,283.84**
Rounded to Nearest $100.00			**$8,600.00**	**+/- $1,300.00**

Observations

If clearer instructions had been provided to the users who needed to change their passwords, then the network service manager may not have needed to contact some individuals twice, thus reducing the cost of the incident.

The computing specialist mentioned that the network service manager was on the brink of retiring and seemed a bit apathetic to the results of this incident. The computing specialist guessed that the network manager was simply biding time until leaving, and, as a result, let the upkeep of his network slip.

It is unknown whether the hacker(s) damaged or stole any files while compromising the accounts. If information was tampered, the costs could be higher in this incident. This should be considered an unquantifiable cost.

In addition, the problem was not fully solved because the perpetrator had stolen an entire password file, but the manager only dealt with the passwords definitely known to have been compromised. Thus, the potential for further break-ins still exists and may result in additional costs in the future.

4. The Exposed SSNs

The Incident and Its Resolution

In March 1997, a system administrator informed the campus information technology ombudsman that a university Web site was openly displaying personal information about past and present faculty members. The site contained a faculty research database that was inadvertently accessible via an obsolete, but still active, gopher-http gateway. The database disclosed information such as the faculty members' full names along with Social Security and office telephone numbers.

By the time the university became aware of the site, a self-described "privacy advocate," from outside the university community had encountered the site and posted the information on his personal Web site. The individual had then contacted several media outlets and affected faculty members to express his concern with the "apparent lack of security concerns at the university."'

Aware of liability issues, the university acted quickly. Information technology technicians removed the Web page while the university administration asked the privacy advocate to remove the personal data from his Web site. Refusing at first to comply with the university's request, the individual acquiesced once the FBI became involved.

Further investigation by university officials revealed that approximately 2,700 individuals were affected by the open gopher-http gateway. Of the 2,700, approximately 1,100 were current faculty; the remainder had either left the university, or were emeriti. Each affected faculty member received a brief letter from the university describing the situation. In response to the media attention the university received, the university involved the media relations department as well as the general counsel.

Costs and Incident Implications

We estimate that the total quantifiable cost of this incident is **$57,500**. This figure includes the wages paid to the information technology, general counsel, and media relations staff, as well as an estimate of the costs to affected faculty members.

This figure does not include the following factors:

- *Issues that our analysis cannot quantify, but that we consider costly to the university.* We have addressed these issues later in this report.

- *The establishment of an information security officer.* Following the incident, the university developed a position for an "information security officer" who is charged with proactive scanning of university networks and incident response. We assume that the inevitability of the position's development precludes it from being considered a true cost of the incident. However, we concede that the incident probably sped the process.

- *An independent audit of the network.* The university contracted an independent security team to perform an audit of the university's networks. Although this audit would probably have taken place at some point, the incident hastened its occurrence.

- *A task force to review policy regarding the use of Social Security numbers.* The university created a task force to investigate the various uses of Social Security numbers around the university. The university is

attempting to move away from the use of Social Security numbers as identifiers and to protect itself from the problems this incident created. Again, we have not included this cost as part of the analysis, but understand the importance of the incident in accelerating the policy change process.

Workers' Costs

In analyzing the costs accrued by the university via wage payments, we obtained the names of the people most involved in the incident's resolution. We multiplied their respective wage rates by the logged hours to obtain an estimate of total workers' costs. Our estimate for university workers' cost is $22,300. For details, see Table C-12.

Table C-12

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Computer Support	25	$82.80	$2,070.00	$1,759.50	$2,380.50
Computer Support	50	$44.80	$2,240.00	$1,904.00	$2,576.00
Computer Support	50	$34.41	$1,720.63	$1,462.53	$1,978.72
Computer Support	50	$15.83	$791.25	$672.56	$909.94
Computer Support	75	$30.81	$2,310.94	$1,964.30	$2,657.58
Counsel1	5	$35.50	$177.50	$150.88	$204.13
Counsel2	25	$55.96	$1,399.06	$1,189.20	$1,608.92
Public Relations	4	$65.36	$261.45	$222.23	$300.67
Public Relations	8	$41.20	$329.60	$280.16	$379.04
Public Relations	12	$14.10	$169.20	$143.82	$194.58
Subtotal	304		$11,469.63	$9,749.18	$13,190.07
Benefits			$3,211.50	$2,729.77	$3,693.22
Subtotal (Salaries + Benefits)			$14,681.12	$12,478.95	$16,883.29
Indirect Costs			$7,634.18	$6,489.06	$8,779.31
Total Labor Cost			**$22,315.30**	**$18,968.01**	**$25,662.60**
Median Costs +/- 15%				$22,315.29	+/- $3,347.30

Costs to Affected Faculty

To analyze the costs to the affected faculty, we developed a profile based on what we believe is the response behavior for affected faculty who are still part of the university. We believe that this method produced a conservative, yet responsible, measure of how much the incident cost those affected.

Each of the 1,100 current faculty members received a letter from the university describing the situation. We assumed that, on average, each individual spent 30 minutes dealing with the letter, writing responses, or making phone calls. We believe this is a conservative estimate based on the potential for personal financial harm from the disclosed data. We then estimated an average wage rate of $30 per hour and used that figure as a basis for

quantifying a faculty member's time. Finally, we multiplied the number of current faculty members by our estimated wage rate. We determined that faculty members spent 550 hours addressing the problem at a cost to the university of $32,100.

Table C-13

Affected Faculty Costs					
Number of Users	Hours	Cost/Hr.	Total	-15%	15%
1100	550	$30.00	$16,500.00	$14,025.00	$18,975.00
Subtotals	550	$30.00	$16,500.00	$14,025.00	$18,975.00
Benefits			$4,620.00	$3,927.00	$5,313.00
Subtotal (Salaries + Benefits)			$21,120.00	$17,952.00	$24,288.00
Indirect Costs			$10,982.40	$9,335.04	$12,629.76
Total Users' Costs			**$32,102.40**	**$27,287.04**	**$36,917.76**
Median Costs +/- 15%				**$32,102.40**	**+/- $4,815.36**

Incidental Costs

A member of the information technology center's staff who was away on business returned to the university when the incident began. As part of his trip, the university had rented studio time to produce educational videos. The unplanned return trip resulted in the loss of the $2,500 rent paid to the studio. Normally, this would not be considered a cost, but because he had to return to finish the work and pay the rental fee again, we consider it a loss. In addition, the quick flight home and shuttle to the airport cost the university an additional $600. Total incidental costs to the university were $3,100.

Table C-14

Incidental Costs	
Flight:	$550.00
Shuttle:	$50.00
Lost studio time:	$2,500.00
Total Incidental Costs	**$3,100.00**

Total Costs

Table C-15 shows the combined quantifiable costs to the university:

Table C-15

Total Costs					
Total Labor Costs				$22,315.29	+/- $3,347.30
Total Faculty Costs				$32,102.40	+/- $4,815.36
Total Incidental Costs				$3,100.00	
TOTAL COSTS				$57,517.69	+/- $8,162.66
Rounded to Nearest $100.00				$57,500.00	+/- $8,200.00

The Unquantifiable Issues

Of the unquantifiable issues, the most problematic is the disclosure of the Social Security numbers and the potential for their misuse. For example, a Social Security number, name, and telephone number are adequate information for a criminal to obtain fraudulent credit cards and telephone accounts. The university has already handled two phone card fraud reports that are likely a result of the disclosed information. A faculty member might have grounds for a lawsuit if a court deemed the university negligent in its protection of private information. With 2,700 affected people, settlements could reach millions of dollars.

The university is dealing with an increased number of intrusion attempts as a result of the media's attention to the incident. Once a system is deemed "open," hacker circles will attempt to break into the network with the potential of creating additional problems for the university. The increased attention by hackers only serves to exacerbate the existing problems.

Another issue that our analysis does not quantify is the potential loss in prestige. If top students or faculty choose not to become part of the institution as a result of the incident, the university will slowly lose its academic reputation. If decreased enrollment or reduced grant or research funding can be traced to negative press, then they must be included as true costs to the university resulting from the incident.

5. Give Him an Inch, He'll Take a Mile

The Incident and Its Resolution

A financial administrator received an e-mail from an external site which suggested that there might be a security problem within his domain and directed him to a referenced URL. The financial administrator found at the site an offer to "download a game client here" and the IP addresses for two of the three servers in his office. IRC ports had been set up to make the software available.

The machines were immediately inspected by auditing managers and two oddities were discovered.

- No logs were running on one of the machines.
- Port scans revealed programs that were completely unrelated to the intended use of the server.

Security personnel suspected that a student system administrator of the three machines was responsible. The machines were taken off line to prevent any further misuse. Personnel attempted to bring up the legitimate systems residing on the machines to allow people access to what they needed. Specific items from the server, however, including downloadable travel forms and other financial paperwork, were unavailable for about three days, mostly over a weekend. When the system was brought back online, however, it created another security hole and was down for another three days. It was estimated that productivity of the potential 200 employees who used the forms declined by 5-7%.

The servers were taken to a Windows NT expert for analysis. The machines were not configured in any typical manner, and the inspection took three weeks. The inspection revealed that:

- The student system administrator was incompetent with Windows NT.
- Employees within the office had privileges and access to information they didn't need.
- Employees had guessable passwords.
- The three servers were set up interdependently, so any change in one broke critical front door procedures on others.
- Public and private information were mixed together.
- There was a file named WAREZ on one machine.

The administrative level of the office was such that highly sensitive data was legitimately available to its employees. The student, however, had failed to secure access to such sensitive items as the digitized signatures of administrative officers, the backup files, or the university's standard policies guide.

A number of recommendations were put forth to secure the office and prevent any further abuse of the systems. Ultimately, the student was fired for incompetence, but never admitted to the creation of the game client site.

Costs and Incident Implications

Our analysis revealed that the incident cost the University **$15,700** to **$29,800**. This figure includes both the workers' costs for investigating and analyzing the servers and an estimate of the users' costs attributable to the downed servers. The uncertainty in estimating user costs is responsible for the range in total costs. A more detailed explanation follows in the "Users' Costs" section.

Of great concern for the computer security personnel was the amount of responsibility and access to information given to the student, especially in light of the highly sensitive data that was legitimately available to the staff. Therefore, the office instituted new polices aimed at curbing these and other potential problems. A full-time professional system administrator was hired to oversee the computing operations. Procedures for information security were developed, and a hierarchy for accessing information was established.

Workers' Costs

Ten university employees investigated and analyzed the incident for a reported 355 hours. We multiplied the reported hours for each employee by the respective salary figure to obtain a total wage cost figure of $15,700. The majority of this cost is attributable to the extensive investigation into the technical setup of the machines. Workers" costs are summarized in Table C-16.

Table C-16

Workers' Costs					
Title	Hours	Cost/Hr.	Total	-15%	15%
Residential Assistant	40	$19.89	$795.46	$676.14	$914.78
Security Director	56	$37.37	$2,092.57	$1,778.68	$2,406.45
Incident Response Analyst	128	$15.25	$1,951.75	$1,658.99	$2,244.52
Audit Manager	24	$21.99	$527.68	$448.53	$606.83
Security	3	$21.98	$65.95	$56.05	$75.84
Network Analyst	40	$17.00	$680.08	$578.07	$782.09
Sr. Financial Adminstrator	24	$45.08	$1,082.01	$919.71	$1,244.31
Unit Specialist	32	$19.89	$636.37	$540.91	$731.82
Asst. Univ. Auditor	6	$36.07	$216.42	$183.95	$248.88
Staff Assistant	2	$16.10	$32.20	$27.37	$37.03
Subtotal	355		$8,080.48	$6,868.41	$9,292.55
Benefits			$2,262.53	$1,923.15	$2,601.91
Subtotal (Salaries + Benefits)			$10,343.01	$8,791.56	$11,894.47
Indirect Costs			$5,378.37	$4,571.61	$6,185.12
Total Labor Costs			$15,721.38	$13,363.17	$18,079.59
Median Costs +/- 15%				$15,721.38	+/-$2,358.21

Users' Costs

A potential 200 university employees downloaded financial forms from the server daily. It is not clear how much each employee was affected, given that the server was offline for six days. Many of these employees kept hard-copy versions of the forms that could be duplicated. Some services, however, could only be used or obtained online.

Given this uncertainty, we developed two sets of scenarios to estimate the monetary value of the productivity loss to users. The first set accounts for the downtime over the weekend, where use is minimal. Based on our investigation, we estimate that approximately an eighth of the potential users were affected. The second set of scenarios accounts for the second three day outage. In both cases, we vary the number of hours lost as a percentage of the total downtime. We estimate that the university lost between $0.00 and $14,000 through the reduced productivity of its users. See Table C-17 for details.

Table C-17

User Costs			
First Outage			
Employees	**Hours lost**	**Hourly Wage**	**Subtotal**
Scenario One	0	$12.50	$0.00
Scenario Two	1	$12.50	$312.50
Scenario Three	2.5	$12.50	$781.25
Scenario Four	5	$12.50	$1,562.50
Second Outage			
Employees	**Hours lost**	**Hourly Wage**	**Subtotal**
Scenario One	0	$12.50	$0.00
Scenario Two	1	$12.50	$2,500.00
Scenario Three	2.5	$12.50	$6,250.00
Scenario Four	5	$12.50	$12,500.00
Estimated User Loss	**$0.00-$14,062.50**		

Total Costs

The total cost to the university from the incident is determined by adding the workers' and users' costs, as shown in Table C-18.

Table C-18

Total Costs				
Workers' Costs			$15,721	+/- $2,358.21
Users' Costs			$0.00 -$14,062.50	
TOTAL COSTS			**$15,700 - $29,800**	**+/- $2,400.00**

Unquantifiable Issues

The following are issues which cannot be quantified explicitly, but should be considered real or potential costs that could result from the incident:

- The ability of unauthorized persons to change the standard practices guide could have resulted in productivity losses when changes were corrected.

- The establishment of the WAREZ site on the servers could have resulted in a costly lawsuit from software companies over copyright infringement.

- The ability of unauthorized persons to obtain the digitized signatures of administrative officers could have resulted in monetary loss.

6. The Horse in the Public Site

The Incident and its Resolution

A school's system administrator and her team noticed that the PC login machines in a student computing site had been compromised. A cursory scan of the machines revealed a Trojan Horse that looked identical to the standard login screen, but saved IDs and passwords on the computer's hard drive. The stored passwords were later retrieved by the perpetrator(s) and copied to a floppy disk. An investigation by the system administrator assured her that the compromised passwords were not being transferred over the network, but at least 75 passwords had been taken from the machines.

Similar Trojan Horses were discovered at other sites and believed to be related to the initial incident. Another 75 passwords appeared to have been stolen for a total of 150. Approximately 75 of the 150 were inactive accounts, as defined by the university's IT accounts office. For the purposes of this analysis, we use 75 as the number of affected users.

The university took immediate action to purge the machines of the Trojan Horses and clean up the affected accounts. The system administrators contacted the information technology ombudsman (ITO) for assistance. The ITO's attempts to contact the individuals with compromised accounts by telephone met with only moderate success. Given the urgency of the situation and the possibility for alteration, destruction, and liability against the university, officials decided to shut down the compromised accounts without further notice to the users.

To restore service to their accounts, students were required to obtain a new password from the computing center administration and have their accounts cleaned by an information technology technician. It was feared that the hacker may have introduced subtle changes to individual accounts that would continue to leave them in a compromised state even after their passwords were changed.

The ITO contacted the campus police department with the intent of apprehending the perpetrator. They considered using false IDs in the sites where the Trojan Horse appeared, in the hope of tracking their reappearance on the login servers. They were concerned, however, that because of the compromised nature of the network, any attempt to apprehend the perpetrator would delay the cleanup efforts. Therefore, they decided to begin cleanup instead.

Costs and Incident Implications

At a minimum, this incident cost the university between **$12,800** and **$21,100**. The cost range results from the uncertainty involved measuring students' time in monetary terms.

The potential exists for additional costs stemming from unquantifiable issues. We address those issues in a later section of this report.

Workers' Costs

Twenty-two university employees were involved in the resolution of the incident. Based on their self-reported log of hours and wage rates taken from university salary publications, we determined that 406.5 hours were spent resolving this incident at a cost to the university of $11,600. (See Table C-19 for details.)

Table C-19

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Technical	11.00	$28.92	$318.12	$270.40	$365.84
Sites Administrator	12.50	$20.48	$256.00	$217.60	$294.40
Technical	35.00	$12.16	$425.60	$361.76	$489.44
Campus Police	4.00	$26.39	$105.56	$89.73	$121.39
Technical	45.00	$18.99	$854.55	$726.37	$982.73
ITO	10.00	$33.17	$331.70	$281.95	$381.46
Administration	1.00	$35.24	$35.24	$29.95	$40.53
Press	1.00	$21.01	$21.01	$17.86	$24.16
ITO	1.00	$11.63	$11.63	$9.89	$13.37
Administration	1.00	$26.59	$26.59	$22.60	$30.58
Press	8.00	$22.36	$178.88	$152.05	$205.71
ITO	40.00	$16.11	$644.40	$547.74	$741.06
Administration	1.00	$72.12	$72.12	$61.30	$82.94
Technical	4.00	$22.59	$90.36	$76.81	$103.91
Technical	10.00	$16.11	$161.10	$136.94	$185.27
ITO	1.00	$30.11	$30.11	$25.59	$34.63
Technical	35.00	$9.00	$315.00	$267.75	$362.25
Campus Police	1.00	$22.74	$22.74	$19.33	$26.15
Administration	1.00	$32.45	$32.45	$27.58	$37.32
ITO	3.00	$14.57	$43.71	$37.15	$50.27
Technical	160.00	$9.00	$1,440.00	$1,224.00	$1,656.00
Press	4.00	$24.04	$96.16	$81.74	$110.58
Technical	6.00	$31.25	$187.50	$159.38	$215.63
ITO	11.00	$17.31	$190.41	$161.85	$218.97
Subtotal	406.50		$5,890.94	$5,007.30	$6,774.58
Benefits			$1,649.46	$1,402.04	$1,896.88
Subtotal (Salaries + Benefits)			$7,540.40	$6,409.34	$8,671.46
Indirect Costs			$3,921.01	$3,332.86	$4,509.16
Total Labor Costs			$11,461.41	$9,742.20	$13,180.62
Median Cost +/- 15%				**$11,461.41**	**+/- $1,719.21**

Users' Costs

Our inability to sample the affected students directly constrained us from developing the most accurate estimate of student loss. However, we have applied a number of assumptions to a costing technique, and offer it as the best possible alternative to speaking to students directly. The following is based on the understanding that students were impacted in two time periods: one in which the student went without service altogether (denial of service) and the other during which the student and technician worked together to clean up the account.

1. We used the student labor market as an allied market to determine the monetary value of a students time. We estimated that the average undergraduate earns $6.00 per hour and used that figure as a measure.

2. We based our calculations on 75 affected students who, according to an information technology survey, use a computer an average of 1.85 hours per day.

3. We estimated that students waited 10 days on average for services to be completely restored.

4. We estimated three hours of additional student and technician time for account cleanup. For the purpose of this analysis, we assumed that affected students did not have alternative access to campus computing or did not avail themselves of it.

To analyze the costs associated with the denial of service for individuals, we multiplied the number of affected users by the total number of hours affected, using the assumptions given above. We then multiplied this number by an average student wage resulting in an estimate for total "denial of service costs"' of $8,300.

True loss to students must reflect the difference between "denial of service costs" and the utility in monetary terms of what they can do with their time instead of computing, that is, their opportunity cost. A student, for example, may be able to spend his or her time studying instead of working on a computer. Some alternatives to computing could provide as much utility as computing itself. If this was true of every student, it would translate into an opportunity cost of $8,300. In other words, the loss of computing resources would cost the students nothing. At the other extreme, there might be nothing that the students could do to provide utility, resulting in an opportunity cost of $0.00; the students would bear the full $8,300. It is unclear where the true cost lies between those limits; thus we reported our quantifiable costs as a specific range. We excluded activities that provided an opportunity cost higher than the monetary value of a student's time because it implies that students would do no computing at all.

The second piece on the user side of the estimate is the users' cost in lost time spent cleaning up their accounts. Again using the given assumptions, we multiplied the number of students by the wage rate for the number of hours affected, rounded the result, and arrived at a total of $1,400. We do not have to consider opportunity cost issues for cleanup costs because students had no choice but to spend time with the technician. We assume that not having an information technology account is not an option.

The results of these calculations are shown in Table C-20.

Table C-20

Users' Costs					
Denial of Service Costs					
Undergraduates	Hours	Cost/Hr.	Total	-15%	15%
75	18.5	$6.00	$8,325.00	$7,076.25	$9,573.75
Subtotal	18.5		$8,325.00	$7,076.25	$9,573.75
Median Cost +/- 15%				$8,325.00	+/-$1,248.75
Opportunity Cost				$0.00 - $8,325.00	
Time Costs of Cleaning up Accounts					
Undergraduates	Hours	Cost/Hr.	Total	-15%	15%
75	3	$6.00	$1,350.00	$1,147.50	$1,552.50
Subtotal	3		$1,350.00	$1,147.50	$1,552.50
Median Cost +/- 15%				$1,350.00	+/- $202.50

Total Costs

The total costs of the incident are calculated by summing the wage costs and user costs, as shown in Table C-21.

Table C-21

Total Costs			
Workers' Costs		$11,461.41	+/- $1,719.21
Denial of Service Costs		$0.00 - $8,325.00	
Account Clenaing		$1,350.00	+/- $202.50
TOTAL COSTS		$12,811.41 - $21,136.41	+/- $1,921.71
Median Cost Rounded to Nearest $100.00		$12,800.00 - $21,100.00	+/- $1,900.00

Unquantifiable Issues

Of the unquantifiable issues, the most problematic for the university is the proliferation of WAREZ sites using the compromised passwords stolen by the Trojan Horse programs. A WAREZ site is a compromised account that the perpetrator(s) uses to distribute copyrighted software illegally. During the cleanup process, WAREZ sites were discovered in a number of the compromised accounts. The university could face charges of copyright violations because of lack of control of its network, with the potential for severe court settlements.

Remember that our method for measuring students' losses fails to account for frustration, stress, inconvenience, and the realistic possibility that a student has an alternative means of computing.

Observations

About one month after the Trojan Horse discovery, the ITO staff met to develop guidelines for dealing with similar situations in the future. The question left unanswered, however, was whether or not the university should attempt to apprehend the perpetrator. If the university decides to go after the hacker, it delays cleanup, but it effectively sends a strong message to hackers.

Alternatively, if the university prescribes immediate cleanup, as it did in this incident, it lowers liability for the university, but doesn't show hackers that the university is in control of its systems. The university must decide which is more important, lowering liability or apprehending the perpetrator(s).

7. The Infamous Hacker Gong

The Incident and Its Resolution

An ISP located in California contacted the senior computing specialist at a university. The ISP reported that someone had broken into one of its computers with an address from the university. The person using the address demanded an account from the ISP and threatened to break in if he was not given one. Since the ISP was talking to him on an IRC, it was able to acquire the nickname he used.

The senior computing specialist checked the address and realized it was a dialup address. Upon further investigation, he discovered that the account being used was compromised. He then looked through his incident database and realized that someone using the same nickname had been involved in four or five prior incidents at the university (for example, break-ins and shutting people out of IRC). This individual had access to several compromised accounts. He decided it was worth the effort to track the perpetrator down.

The senior computing specialist called the phone company to place a trace on the phone line. The process, which he thought would take a matter of minutes, turned out to take about six months.

Since there was such a delay with the phone traces, the senior computing specialist decided to log the network traffic that was using the compromised accounts. He was able to watch more and more of the hacker activity. He discovered that it was not just one hacker causing problems, but at least ten hackers who shared accounts. He also discovered new accounts that they were using. During this time, he collected 20 gigabytes of log files and spent roughly half his total time over a year reading the log files. (The 20 gigabytes of log files represented only 25 to 50 percent of the hackers' activity.)

A major factor of this incident is the lengths that the senior computing specialist went to in order to investigate the incident. Instead of putting the incident on hold for six months until the phone company installed the traces, he decided to track the activities. If he had not begun logging the files, he would never have received the amount of incriminating information that he did. He discovered that this group of ten hackers were part of an even larger group(s) consisting of between 20 and 30 hackers.

While tracking the activity of the hackers, he noticed that one of them was scanning for Web sites with "phf" bugs. The hacker posted on a Web site a request for known sites with "phf" bugs and received many lists of Web sites back from various Internet users. He tried them all and posted the flaws and holes of each site.

The same individual broke into military sites. This caused major concern to the FBI, the Navy, and the Air Force. None of the sites was classified, but any breach into a military site is a serious matter. This activity brought the incident to a higher, federal level.

One of the ten hackers began bragging on an IRC about an expensive computer system he had in his home. The senior computing specialist, who was observing the chat at the time, remembered that four expensive computers were stolen from one of his university's computing sites. From the description in the log files, it sounded like the same type of system. Additionally, he remembered that four or five people were caught trespassing within the underground tunnel system, but were not charged. This tunnel system connects to the computing site. Upon questioning, it was determined that the hackers had stolen the computers and had stored them in the tunnels to pick up at a later time. When he went with his friends to pick them up the first time, they were caught by security. They simply returned at a later date to retrieve the equipment.

It took a year for search warrants to be issued for the ten hackers. These ten hackers will be charged at both a state and federal level. They were not students from the university; therefore no action was taken at a university level. The other hackers in the gang were not doing enough malicious activity to warrant an investigation.

Implications for Users

This incident provided unique insights into hacker activities. By investigating the hackers without their knowledge, the senior computing specialist was able to see what really is going on in the world of the hacker. It was much more informative than the information that is received from "born again hackers."

The incident shed a harsh light on just how sensitive the computer labs are and how exposed the university is to great liability. It is possible for hundreds or thousands of systems to be compromised. The incident has helped underscore the need to protect account security by reducing the threat of sniffing, break-in, and so on.

New software or hardware will not be purchased as a result of this incident. However, the university has decided to replace all hubs with switches, which will no doubt help ward off any attacks similar to this one. Since they were planning to implement this action eventually, it is not considered a direct cost of the incident. They are also considering establishing a password program, which may include a system that will issue account activity statements, probably electronically. This has not yet been implemented and, again, would probably have been done even if the incident had not occurred, so the system is not included in incident costs.

Account management procedures are changing as a result of the incident. Education on passwords will be implemented as well. Several of the accounts that were compromised had the original passwords that were assigned to them when they were established. If the users had changed their passwords, and changed them often, it is probable that those accounts would not have been compromised.

As a direct result of this incident, a system has been created to log and monitor activity. The computing specialist wrote a software program to go through the log files that can be used for future situations. If he had not written the software, he would have never been able to get through the amount of information that he did.

A major problem that probably contributed to the incident was that security features were not turned on in many of the hubs. This could be due to lack of awareness on the part of the computer monitors, or possibly laziness. All security features are now turned on.

If the security features had been turned on, some of the damage may have been avoided. This is a knowledgeable group of hackers, however, who have broken into many different sites. Even with the security features on, they may have found other ways to enter the system.

Costs and Incident Implications

Our analysis reveals that this incident cost the university an estimated **$150,100**. This figure includes both the significant workers' costs as well as costs associated with the lost equipment, which was positively identified as being stolen by the perpetrators.

Workers' Costs

We determined that the total workers' costs for this incident were $126,000. Employees spent 3,790 hours resolving the incident. The senior computing specialist, who was in charge of investigating the incident, chose to invest that time for a number of reasons. He decided that he wanted to pursue this incident to the end, even if

it took him the better part of one year to do so. The desire to pursue the perpetrators was not out of a sense of revenge, or due to a lack of anything better to do. Rather, the senior computing specialist wanted to let this hacker gang, as well as others, know that his university was not the best place to invade in the future. He also learned a staggering amount of information about the hacker community in general, which he has shared with fellow universities. Our findings are detailed in Table C-22.

Table C-22

Workers' Cost					
Title	# of Hours	Cost/Hr.	Total	-15%	15%
Sr. Comp. Specialist	1160	$31.25	$36,250.00	$30,812.50	$41,687.50
Detective	550	$26.44	$14,542.00	$12,360.70	$16,723.30
Graduate Assistant	2080	$6.73	$13,998.40	$11,898.64	$16,098.16
Subtotal:	3790		$64,790.40	$55,071.84	$74,508.96
Benefits @ 28%:			$18,141.31	$15,420.12	$20,862.51
Subtotal (Salaries + Benefits):			$82,931.71	$70,491.96	$95,371.47
Indirect Cost Rate (52%):			$43,124.49	$36,655.82	$49,593.16
Total Labor Cost:			**$126,056.20**	**$107,147.77**	**$144,964.63**
Median Cost +/- 15%			$126,056.20	+/- $18,908.43	
Rounded to Nearest $100.00			$126,000.00	+/- $18,900.00	

Equipment Costs

As stated above, the senior computing specialist determined that the hackers had stolen four expensive computers from a computing lab. All four computers had been replaced at a total cost of $24,000. Details are found in Table C-23.

The discovery of the link to a physical theft increased the costs of this incident, as well as identified charges on which the hackers could be arraigned.

Table C-23

Equipment Cost			
Description	# of Units	Cost/Unit	Total
Stolen Computers	4	$6,000.00	$24,000.00
Subtotal			$24,000.00

Total Costs

To arrive at the overall cost of the incident, we added the subtotals of the workers' and equipment costs of the incident. See Table C-24 for details.

Table C-24

Total Costs		
Workers' Cost	$126,056.20	+/- $18,908.43
Equipment Cost	$24,000.00	
Total Costs	**$150,056.20**	**+/- $18,908.43**
Rounded to Nearest $100.00	**$150,100.00**	**+/- $18.900.00**

Unquantifiable Costs

This incident is still ongoing. Therefore, we were unable to include the cost of bringing the hackers to trial to the university. The incident ballooned to include federal and state investigators. Though we do not include costs accrued by investigators not related to the university, the involvement of these federal and state investigators with the investigators at the university increased costs due to ongoing consultations and meetings. Thus, the cost of the incident to the university could very well exceed our figure of $150,100.

Whether or not the hackers damaged or deleted files while compromising accounts is unknown. If they did, repairing or reproducing these files would be considered a real cost to the university. It is important to keep this in mind when examining incidents such as this.

Incident Implications

The main reason for the high cost of the incident is the number of hours spent investigating. Other institutions may not have attacked this incident so vehemently. However, this institution wanted to take a strong stance against the hacker community. Since this hacker gang consisted of approximately 20 to 30 hackers, it can be assumed that all know of the incident and will probably never snoop around that university again. If those hackers tell their hacker friends, who tell their friends, and so on, then a reputation is formed and this institution is respected as one who will crack down against hacker intrusions in the future.

It is important to highlight that this approach, with its associated costs, was chosen by the institution. The senior computing specialist could have put the incident on hold for six months while waiting for the phone traces. Because he chose not to do so, and instead logged and monitored the activity carefully, not only did he determine the identity of the hackers, but he also solved the mystery behind the missing equipment.

8. The Interrupted Uninterruptible Power Source

The Incident and Its Resolution

The incident involves the failure of one of five uninterruptible power sources (UPSs) at one of the university's computing centers. These building-wide UPS systems are about 30 years old and have passed their working lifetime. Therefore, they are not as reliable as they should be. One of the three people called to the scene to repair the system is one of a very few people who knows anything about this UPS -system. Documentation and training are out of date.

The power outage lasted about 50 minutes. During this outage, connectivity was lost for the following:

- **CICnet connections fed out of the city**
- **Various state-wide network connections**
- **The following connections on the campus:**
    - All connections to off-campus university buildings
    - ISDN dial-in pools
    - The network at one of the information technology office's sites
    - Netware file and print services provided by the information technology office
    - Network connection to the university's purchasing system

During the outage, the following services were down:

- **University password authentication servers**
    - Authentication for IMAP service
      (result: users couldn't access electronic mail)
    - Authentication for both analog and ISDN dial-in university users
      (result: users couldn't dial into the network)
    - Authentication for access to campus computing site machines
      (result: users couldn't log in on the campus site systems)
    - Authentication for ARA over TCP service
      (result: users couldn't access AppleShare files when dialing in)
- **Domain Name Service for University**

  Users could not specify a domain name to reach services, just IP addresses.

- **Institutional File System (IFS)**

  Users lost access to home directories and their shared files space.

- **Automated Billing System (ABS)**

  Due to this service being out, other services, such as dial-in and printing, were unusable because those services need to check users" account balances to verify that the user can pay for service or to record billing information.

- **General Purpose Computing machines (login machines)**

  These are the machines most university faculty, staff, and students use for email and other general computing services.

Services that were affected beyond the duration of the outage are as follows:

- **IFS**

  It took 22 hours to get IFS back up and running. Thus, the login service was virtually useless. The only users that were unaffected by the unavailability of this service are those whose accounts were hosted within a specific department.

- **ABS**

  It took 22 hours to get ABS back up and running. With ABS down, users were not able to dial in or print at a campus computing site. The only possible exception was people who used a PPP connection to dial in.

- **General Purpose Computing machines (login machines)**

  One login machine had memory problems because of the outage, which took two days to be resolved. Since the login service is run on a pool of eight systems, losing one is not a major problem. Users may have had temporary problems connecting, but no one would have been shut out.

The most detrimental effect of the outage was the extended outage (more than 24 hours) of several AFS services. The AFS outage was not immediately detected, and thus, it took some time to inform the necessary individuals of the problems so that they could begin to resolve the incident.

One technologist spent most of his time checking about 150 disk drives for damage. It took about six hours to get all but one file server going again. That server had a disk that worked, but was obviously failing, so he spent time moving the data to another server. In his opinion, he could have sped up many of the procedures for getting the systems back up, but he had not had the chance to test his ideas and did not want to try them on production systems without testing.

The same technologist had a difficult time getting ABS going since one of the programmers had changed a startup file. He spotted the change and, assuming that there was a reason for it, waited to talk to one of the

programmers before doing anything. Unfortunately, one programmer was out of town, and the others were unavailable for almost 24 hours after the incident occurred.

A Web services programmer spent a great deal of time working on problems with Web servers. All but one of the five Web servers started back up when the power came on. The one that did not, however, is the one that had custom applications on it, and the recovery involved hours of attempting to retrieve the custom applications. The unavailability of this server affected all Intranet services supplied by this university.

Costs and Incident Implication

Our analysis shows that this incident cost the university at the very least **$4,700**. We believe that this figure is a gross underestimate of the actual costs of the incident because we were unable to determine the users' costs associated with this incident. (For more information, see "Unquantifiable Costs" later in this report.)

Workers' Costs

Seven employees reported working on this incident for 107 hours, resulting in a total wage cost of $4,700. The details of the wage costs can be found in Table C-25.

Table C-25

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Technologist	20	$29.18	$583.60	$496.06	$671.14
Elec. Technician	2	$19.26	$38.52	$32.74	$44.30
Technologist	12	$23.17	$278.04	$236.33	$319.75
Technologist	10	$30.56	$305.60	$259.76	$351.44
Webmaster	30	$17.25	$517.50	$439.88	$595.13
Associate Director, IT	3	$46.25	$138.75	$117.94	$159.56
Webmaster	30	$17.66	$529.80	$450.33	$609.27
Subtotal:	107		$2,391.81	$2,033.04	$2,750.58
Benefits @ 28%:			$669.71	$569.25	$770.16
Subtotal (Salaries + Benefits):			$3,061.52	$2,602.29	$3,520.74
Indirect Cost Rate (52%):			$1,591.99	$1,353.19	$1,830.79
Total Labor Cost			$4,653.51	$3,955.48	$5,351.53
Median Cost +/- 15%			$4,653.51	+/- $698.03	
Rounded to Nearest $100.00			$4,700.00	+/- $700.00	

Unquantifiable Costs

It is impossible to determine the number of users who were affected by the failure of the UPS. Approximately 80,000 users use the services that were affected. However, the UPS failure occurred on a Saturday during a

holiday break. We received no records indicating the number of users using the affected systems immediately before the incident, and thus have no numbers to go by.

Therefore, we have decided not to try and quantify the users' costs associated with this incident. It can be assumed, however, that even considering the fact that the power failure occurred on a holiday break, the costs far exceed the workers' costs associated with re-establishing the system.

9. The Invasion of the Body Swappers and Other Horrors

The Incident and Its Resolution

Six incidents occurred in this information technology (IT) support office in a four- to six-month period. We cannot determine whether or not these incidents are interrelated. The incidents are labeled A through F.

Description and Resolution of Incident A

This university participates in a software select pricing program offered by a leading software manufacturer. As a member of this program, the university, by meeting certain requirements such as purchase volume, receives this normally expensive software at very reasonable prices

One of the student workers in the office was given the CD-ROMs for the software programs and instructed to install them on a university server. After completing the installation, he returned them to a staff mailbox without putting them in an envelope or attempting to conceal them in any way. He returned the disks to the mailbox at 3:30 a.m.; by 8:45 a.m. the next morning they were gone.

Thanks to the special pricing program, the actual cost of the software to the university was minimal. The theft, however, placed at risk this beneficial program, which saves the university thousands of dollars. It was extremely detrimental to have these CD-ROMs unaccounted for because there was nothing to stop the thief from installing these very expensive programs anywhere he or she wanted. It placed the university's reputation in jeopardy and could deter future partnerships with the corporation.

The building in which the theft took place is a 24-hour facility; however, the room where the mailboxes are located was secured by a special security system. The only people who had access to the room were the student workers and the full-time staff members. The manager acknowledges that the perpetrator may have been someone who worked in the office itself or may have accompanied someone who had a key to the office.

The manager reviewed the security system records for 3:30 a.m. to 8:45 a.m., but it was impossible to determine the perpetrator solely from the records. At this point the police were not called.

Description and Resolution of Incident B

The same weekend that Incident A occurred, the same student employee was testing a new, high-end Toshiba laptop computer and a PC Ethernet card. The laptop was on loan to the department for inspection from the university's computer store. Another staff member borrowed the laptop and returned it to the office. The student worker saw it sitting in the open on a desk and decided to place it in a drawer within the student employee work area, thinking it would be safer. When he went to get it out of the drawer after the weekend, it was gone.

The police were called, who immediately involved their detective. A manager reviewed the security records to try to determine if anyone was in the area who shouldn't have been. Two people were interviewed. The detective and managers suspected that student employees were responsible, but they had no proof. Because it appeared to be an inside job and they wanted to treat the situation delicately, the detective decided that, if the equipment was returned, they wouldn't prosecute. Nothing was returned.

Description and Resolution of Incident C

In the same student working area, someone switched the CPU of a PowerMac 6100 with that of a Quadra 610. (The two machines have the same size outer casing.) He or she then took the PowerMac 6100, disguised as a Quadra 610. Later, the same student worker from incidents A and B discovered that the computer was running rather slowly, but he didn't investigate. The computer then got transferred to another student group. While they tried to install software on it, they received repeated messages that they were trying to install PowerMac software on a machine that wasn't a PowerMac. One of the repair technicians opened up the machine and immediately discovered the Quadra CPU.

To get access to the PowerMac to perform the switch, the perpetrator needed access to the security system. It was impossible to determine when the switch happened, so checking the security records would have been useless. They tried to trace the serial number of the Quadra. to see if they could determine its previous owner, but the serial number was never registered.

Description and Resolution of Incident D

Occasionally, the manager's senior student employees take Ethernet cards from the office to perform checks on machines that may have bad Ethernet cards. The manager has supplied the student workers with a wide variety of Ethernet products to use as needed. Sometime during the late Spring, the manager discovered that someone had substituted an ISA Ethernet card for a brand-new PCI Ethernet card inside the new Ethernet card box. The manager was concerned, but not enough to call the authorities.

The manager talked to her staff about it, however, explaining to them how stealing equipment from the office affects the workplace as a whole. The manager then asked that, if anyone knew who may have stolen the new Ethernet card, he or she should encourage the person to return it. The following Monday, the card was stuffed in the manager’s mailbox. No loss occurred.

Description and Resolution of Incident E

Whenever the manager went out of town, she found certain items missing from her office when she returned. The first time she noticed anything was gone, three new Ethernet Farallon cards were missing. She determined that whoever was breaking in must have had access to her schedule; therefore, it was probably an inside job. Although the missing items were not locked up within the office, the door to her office was supposed to be locked at all times, except when support staff needed to retrieve items from the office.

What disturbed her most was not that the hardware was missing, but that entrance to any office required a special staff key, which was never issued to students. Therefore, either the thief was a staff member, had illegal access to a spare key, or gained access because a staff member left the door unlocked. Investigators were not yet called.

Description and Resolution of Incident F

A couple of weeks after incident E, the manager attended a conference. Three laptop computers were in carrying cases on the floor of her office. When she returned, none of the carrying cases were missing. She even picked up the cases to feel if any were empty; none were.

Two days after returning, she opened one of the cases in order to check out the laptop to a student. She discovered that someone had substituted the Powerbook 5300 in the case with an old Duo. The Powerbook 5300 was the department's best machine. Its loss was detrimental to the office as a whole.

The manager consulted with the detective, who dusted for fingerprints and interviewed people who may have been in the area. They enhanced the security system, installed monitors around certain areas in the building, and, unbeknownst to most of the staff, installed a hidden camera in the manager's office. They also planted a device in the laptop so that if the bags were moved, an alarm would go off at the university's police office. The perpetrator was never caught, although there was one false alarm. A couple of students innocently wanted to use the laptop for training purposes, and a staff member gave them access to the manager's office to retrieve it. They triggered the alarm and were apprehended by police. This false alarm notified all employees that aggressive measures were being taken to secure equipment in the offices.

Costs and Incident Implications

Our analysis shows that this incident cost the university an estimated **$36,400**. The majority of these costs represent the missing equipment that needed replacement, along with the added security measures implemented as a direct result of the incident.

Workers' Costs

Three employees worked for 118 reported hours on these incidents. Based on the hours reported to us, we multiplied the employee wage rate by the total hours worked for each individual. The total workers' cost for this incident is $5,600. Table C-26 depicts our findings.

Table C-26

Workers' Cost					
Title	Total Hours	Cost/Hr.	Total Wages	-15%	15%
Manager	40	$26.44	$1,057.60	$898.96	$1,216.24
Computing Coordinator	40	$24.03	$961.20	$817.02	$1,105.38
Police Officer	38	$22.00	$836.00	$710.60	$961.40
Subtotal:	118		$2,854.80	$2,426.58	$3,283.02
Benefits @ 28%:			$799.34	$679.44	$919.25
Subtotal (Salaries + Benefits):			$3,654.14	$3,106.02	$4,202.27
Indirect Cost Rate (52%):			$1,900.15	$1,615.13	$2,185.18
Total Labor Cost:			**$5,554.30**	**$4,721.15**	**$6,387.44**
Median Cost +/- 15%			**$5,554.30**	**+/- $833.14**	

Equipment Costs

Most of the costs associated with this incident reflect the cost of replaced equipment. Table C-27 lists the costs and descriptions of the equipment that was stolen.

Table C-27

Equipment Costs	
Equipment	**Cost of Equipment**
Laptop computer	$4,000.00
Ethernet card	$200.00
CPU	$800.00
3 Farallon cards	$600.00
Laptop computer	$2,000.00
Ethernet	$110.00
Modem	$225.00
Subtotal	**$7,935.00**

Additional security measures were implemented as a result of these incidents. These costs are displayed in Table C-28.

Table C-28

Security Costs	
Equipment	**Cost of Equipment**
Furniture Safety Features	$400.00
Security Cameras	$5,000.00
Security System	$17,500.00
Subtotal	**$22,900.00**

The total of all equipment costs is listed in Table C-29.

Table C-29

Equipment Total	
Equipment Subtotal	$7,935.00
Security Subtotal	$22,900.00
Total	**$30,835.00**

Total Costs

We arrived at the total cost of the incidents by simply adding the total labor costs to the total equipment costs. These figures are detailed in Table C-30.

Table C-30

Total Costs		
Total Labor Costs	$5,554.30	+/- $833.14
Total Equipment Costs	$30,835.00	
Total Cost	$36,389.30	+/- $833.14
Rounded to nearest $100.00	$36,400.00	+/- $800.00

Implications

The perpetrator(s) of these incidents were never caught. These incidents seem to indicate that there was an abuse of trust among one or more student employees in the office. The computing coordinator acknowledges that she placed a lot of trust in her employees, who were mostly students. She realizes that for many reasons, this was probably not a good idea. First, the students employed tend to be "computer fanatics'" who are fascinated with the equipment. Also, student employees have a high turnover rate associated with the school year. This factor does not allow much time for student employees to develop a sense of loyalty to the office. Of course, the coordinator recognizes that the perpetrator(s) may not have been students at all.

While waiting for the equipment to be replaced, the office staff had to use slower, older equipment in order to complete tasks. This is a cost to the university that could not be quantified, but it still a real cost.

Measures have been taken to improve the physical security of the offices. New furniture is being installed, and everything will be cabled into a locking system. Also, the manager has moved into a different office and keeps all equipment in a locked cabinet within her locked office. Only a limited number of people have access to the cabinet, including a few students who need to be able to access the equipment at times when the manager is unavailable.

The coordinator's general trust level has fallen considerably since these episodes, and she feels that may have hurt the office more than anything, including the missing equipment and the costs of the incidents. The lack of trust that now exists in the office has placed added stress on her and the other office employees. The psychological costs, according to the coordinator, outweigh the actual monetary costs of these incidents.

10. The Juvenile Delinquent

The Incident and Its Resolution

A system administrator received a report from a local Internet Service Provider (ISP) that a break-in had occurred from a departmental machine at the university. Upon investigation, university personnel discovered a lot of unusual activity on that machine. It became apparent that someone was using the departmental machine to break in to other sites.

A research scientist in the department initially tried to close up the security holes in the machine, but the hacker repeatedly broke in. At one point, the hacker erased most of one user's files (for which the department fortunately had backups).

During this time, they monitored the hacker's activity to aid in detecting his real identity. Eventually, they determined that he was a juvenile who had allegedly broken into over a thousand different computers. The case was picked up by the FBI and was pursued at the federal as well as at the state level.

The activity took place on a UNIX mail server, which contained mail and files, as well as programs in regular use, such as Framemaker. The mail was the critical service, as the files and applications were generally available on other platforms. However, some of the special applications were prototype expert systems for which there were no other executable copies.

They had to shut off the UNIX server for almost two weeks in order to replace it with a NT server. This caused a denial of access for all who usually used the server. Mail service and the special applications were essentially shut down for two weeks.

Although the NT server would have replaced the UNIX server eventually, it probably would not have happened so quickly if not for this incident. One incident handler said that the department was much happier with the UNIX mail software. They could not afford anything very expensive for the NT machine and wound up with Ntmail, which is acceptable, she stated, but has caused some problems of its own.

Costs and Incident Implications

Our analysis reveals that this incident cost the university an estimated **$19,100**. This figure includes both the significant workers' costs as well as costs to users while changing passwords.

Workers' Costs

Four university employees were involved in the resolution of the incident. Based on their self-reported log of hours and wage rates taken from university salary publications, we determined that 320 hours were spent in the resolution at a cost to the university of $19,000. Our figures appear in Table C-31.

Table C-31

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Research Scientist	120.0	$21.63	$2,595.60	$2,206.26	$2,984.94
Assistant Professor	120.0	$31.73	$3,807.60	$3,236.46	$4,378.74
Sr. Comp. Specialist	40.0	$31.25	$1,250.00	$1,062.50	$1,437.50
Assoc. Prof/Comp. Sci Chief	40.0	$52.88	$2,115.20	$1,797.92	$2,432.48
Subtotal:	320.0		$9,768.40	$8,303.14	$11,233.66
Benefits @ 28%:			$2,735.15	$2,324.88	$3,145.42
Subtotal (Salaries + Benefits):			$12,503.55	$10,628.02	$14,379.08
Indirect Cost Rate (52%):			$6,501.85	$5,526.57	$7,477.12
Total Labor Cost:			$19,005.40	$16,154.59	$21,856.21
Median Cost +/- 15%				$19,005.40	+/- $2,850.81

Users' Costs

Four faculty and staff members had to change their passwords as a result of this incident. It is estimated that the average wage cost for the faculty and staff members is approximately $30 an hour. It was also estimated that users had to spend approximately fifteen minutes to change each password. The user costs for faculty and staff accrued while changing passwords are $58.37. Please see Table C-32 for details.

Table C-32

Fac/Staff Users' Costs (changing passwords)					
# of Faculty/Staff	Hours	Cost/Hr.	Total	-15%	15%
4	1	$30.00	$30.00	$25.50	$34.50
Benefits @ 28%:			$8.40	$7.14	$9.66
Subtotal (User Costs + Benefits):			$38.40	$32.64	$44.16
Indirect Cost Rate (52%):			$19.97	$16.97	$22.96
Total Fac/Staff User Costs :			**$58.37**	**$49.61**	**$67.12**
Median Costs:				$58.37	+/- $8.76

Six students were also required to change their passwords as a result of this incident. We used a cost rate of $6.00 per hour and estimated that each student spent fifteen minutes on the password changing process. Benefits

and indirect cost rates were not figured into the tabulation of these costs because the students were not employees of the university. It cost $9.00 for the six students to change their passwords. Refer to Table C-33 for details.

Table C-33

Student Users' Costs (changing passwords)					
# 0f Students	Hours	Cost/hr.	Total	-15%	15%
6	1.5	$6.00	$9.00	$7.65	$10.35
Total Student Users' Costs:			$9.00	$7.65	$10.35
Median Costs:				$9.00	+/- $1.35

We then simply added the faculty and staff costs to the student user costs to determine that the total user cost for this incident is $67.37. Please see Table C-34 for details.

Table C-34

Total Users' Cost				
Fac/Staff Users' Costs:			$58.37	+/- $8.76
Student Users' Costs:			$9.00	+/- $1.35
Total Users' Costs:			$67.37	+/- $10.11

Total Costs

By adding the total workers' costs to the total users' costs, we determined the total cost of the incident to be $19,100. Details are in Table C-35.

Table C-35

Total Costs				
Total Workers' Costs			$19,005.40	+/- $2,850.81
Total Users' Costs			$67.37	+/- $10.11
Total Costs			$19,072.77	+/- $2,860.92
Rounded to Nearest $100.00			$19,100.00	+/- $2,900.00

Unquantifiable Costs

Users were without their departmental e-mail server for 2 weeks. However, there were other e-mail servers on campus that they were using, but mail addressed specifically to that address was probably negatively affected

during that time. Though they could still use e-mail on other servers, there is still a cost that needs to be considered due to inconvenience and frustration. Unfortunately, these costs are unquantifiable.

11. LAN Crash

The Incident and Its Resolution

Day One

One morning, when staff members in an administrative office tried to start the four-month-old departmental server, the server would not boot up. Staff members tried all known tricks of the trade to resolve the problem, but the server still would not boot. They then ran a diagnostic program provided by manufacturer. The results of the diagnostic test indicated that no errors were present. When they phoned the manufacturer about the problem, they were told to bring down the server and reload the software.

The department staff wanted a second opinion before resorting to such drastic measures, so they phoned another manufacturer. That manufacturer also told them to reformat the disks and reload the software. They were left with no other choice but to reformat and reload.

That evening they started the reload and got the operating system running. Then around 2:00 a.m., they began reloading the data. The company that manufactured the backup tape system they were using, TapeWare, had gone out of business. The department was in the process of installing a new backup system.

Day Two

The reloading of the data appeared to be "strange," in the words of one employee working on the resolution of the incident. The next day, the department contacted the campus TapeWare expert for advice. They then began the migration process from the old server to a new server, which ran very slowly on the department network. The migration failed. They determined that the old server needed many runs of VREPAIR to be usable. Later in the evening, after staff members went home, they restarted the migration. They created a private network and processing time improved. The VREPAIR process repaired the files.

Day Three

On this day, the staff discovered that the Network Loadable Module (NLM) had become unloaded and that communication from the server to the backup had stopped working sometime within a five-week period. The tape backup logs reported that the backups were successful, but in fact the server was not being backed up.

Late in the afternoon, the migration was completed. During the migration process, the department lost six months of information. The new server was based on a Windows 95 operating system. The old server, and all the data on that server, was not. Therefore, they started configuring the old server environment to match the new server's Windows 95 environment; the configuration had to be done manually. At around 8:00 p.m. that evening, they canceled the tape restore process because the backup software kept reporting that backup was successful, but when they double-checked for themselves, they saw that, in fact, it was not.

Day Four

At this point they had restored the server back to "normal" with files that were dated six months prior. Some department staff members could use the outdated information to recreate new data files for immediate use. Some other staff members had hard copies of the data needed to complete their work and used those to get by. Everyone within the department was affected due to the process of recreating files.

Day Five

The incident handlers spent this day continuing configuration cleanup. They also started to restore data on a system containing student information documentation, which is crucial to the office's operation. They received the permanent archive tape from TapeWare; it was marked "unreadable"' and dated nine months prior to the incident.

Day Six

While trying to restore the student information documentation data, the incident handlers discovered that the outdated tapes that were available to them did not contain the whole system of the documentation. A different backup system called Emerald had been used to back up the student information documentation system prior to the installation of TapeWare. Once it was decided that TapeWare would be used, the information had been transferred onto TapeWare tapes and the Emerald system had been discarded. To get the information from the Emerald tapes, the incident handlers needed a tape drive that would successfully read the old Emerald tapes. They located an Emerald tape drive, but it would not read the backup tapes because it wasn't the same type of system. They were able to find a set of tapes that had some readable information and were able to retrieve some of the data; however, this data was 18 months old.

Days 7-14

The incident handlers found and borrowed Emerald system components and completed the student information documentation data restore from the old Emerald tapes. They then tried every tape in tape inventory, starting with the newest tapes and working backwards, to try to get any data they could. They were unsuccessful with all the TapeWare tapes. The best tapes were those with previous tape backups of separate student information documentation servers.

Four Months Later

The incident handlers noticed a strange error message from the server. Not wanting to take any chances for a repeat of the previous situation, they phoned the manufacturer immediately and demanded that someone physically come to the office and take a look at the server. The manufacturer basically gutted the server, replacing the motherboard, disks, disk array controller, and backplane. The only things left intact were the memory and the power supply. This process was done by the end of the month. The manufacturer never offered a conclusive diagnosis.

A few days later, two drives were simultaneously unavailable for almost four hours. The incident handlers went into the utilities and forced them back. After everything was updated on the disk drives and disk array controller, the server would still not pass the consistency test. They demanded a new server from the manufacturer. Until it arrived, they backed up their information every four hours.

Costs and Incident Implications

Our analysis revealed that the incident cost a total of **$92,500**. This figure includes the workers' costs, the cost to recover items that were lost as a result of the incident, and the new equipment purchased.

Workers' Costs

Nine employees were involved in resolving the incident. These employees logged a reported 288 hours in resolution time for a total cost of $21,000. The salary information for employees 5 through 9 was given to us as averaging $35 an hour. Please refer to Table C-36 for details.

Table C-36

Workers' Cost					
Title	# of Hours	Cost/Hr.	Total	-15%	15%
Info Technologist 1	68	$24.52	$1,667.36	$1,417.26	$1,917.46
Info Technologist 2	55	$19.71	$1,084.05	$921.44	$1,246.66
Info Technologist 3	33	$13.94	$460.02	$391.02	$529.02
Info Technologist 4	60	$23.08	$1,384.80	$1,177.08	$1,592.52
Info Technologist 5	72	$35.00	$2,520.00	$2,142.00	$2,898.00
Info Technologist 6	50	$35.00	$1,750.00	$1,487.50	$2,012.50
Info Technologist 7	30	$35.00	$1,050.00	$892.50	$1,207.50
Info Technologist 8	15	$35.00	$525.00	$446.25	$603.75
Info Technologist 9	10	$35.00	$350.00	$297.50	$402.50
Subtotal:	288		$10,791.23	$9,172.55	$12,409.91
Benefits @ 28%:			$3,021.54	$2,568.31	$3,474.78
Subtotal (Salaries + Benefits):			$13,812.77	$11,740.86	$15,884.69
Indirect Cost Rate (52%):			$7,182.64	$6,105.25	$8,260.04
Total Labor Cost:			**$20,995.42**	**$17,846.10**	**$24,144.73**
Median Cost +/- 15%			**$20,995.42**	**+/- $3,149.31**	

Recovery Costs

Employees spent 1,041.5 reported hours recovering data that was lost as a result of the incident. These employees were paid an average of $35 an hour while recovering the data. The total cost of data recovery was $70,900. The descriptions of the recovery items have been made generic in order to protect the anonymity of the institution. Results of our findings can be found in Table C-37.

Table C-37

Recovery Items					
Description	Hours Spent	Cost/Hr.	Total	-15%	15%
Accounting System	100	$35.00	$3,500.00	$2,975.00	$4,025.00
Project Plans	9	$35.00	$315.00	$267.75	$362.25
Paper Inventory	8	$35.00	$280.00	$238.00	$322.00
Records Directory	40	$35.00	$1,400.00	$1,190.00	$1,610.00
Communications Documents	5	$35.00	$175.00	$148.75	$201.25
Process Documents/Flowcharts	8	$35.00	$280.00	$238.00	$322.00
Process Description	1	$35.00	$35.00	$29.75	$40.25
User Documentation	40	$35.00	$1,400.00	$1,190.00	$1,610.00
Technical Documentation	30	$35.00	$1,050.00	$892.50	$1,207.50
Inventory Database	3	$35.00	$105.00	$89.25	$120.75
Print Project	6	$35.00	$210.00	$178.50	$241.50
Conversion Tallies	2	$35.00	$70.00	$59.50	$80.50
Contact List #1	1	$35.00	$35.00	$29.75	$40.25
Planning Sub-Directories	4	$35.00	$140.00	$119.00	$161.00
Planning & Budgeting Process Manual	40	$35.00	$1,400.00	$1,190.00	$1,610.00
Project Proposal Forms/Instructions	10	$35.00	$350.00	$297.50	$402.50
Project Proposals - Masters	5	$35.00	$175.00	$148.75	$201.25
Project Proposals	5	$35.00	$175.00	$148.75	$201.25
Meeting Information	5	$35.00	$175.00	$148.75	$201.25
Process Team - Masters	4	$35.00	$140.00	$119.00	$161.00
Operations Training Prog, Masters	24	$35.00	$840.00	$714.00	$966.00
Team Budget	1	$35.00	$35.00	$29.75	$40.25
PDPs	15	$35.00	$525.00	$446.25	$603.75
Transcript Process Overview	3	$35.00	$105.00	$89.25	$120.75
Statistics Report	3	$35.00	$105.00	$89.25	$120.75
Technical Design Changes - Document	2	$35.00	$70.00	$59.50	$80.50
Year 2000 Changes	25	$35.00	$875.00	$743.75	$1,006.25
New Issue Directory	3	$35.00	$105.00	$89.25	$120.75
Contact List #2	3	$35.00	$105.00	$89.25	$120.75
Planning Documents	1	$35.00	$35.00	$29.75	$40.25
Environment Documentation	2	$35.00	$70.00	$59.50	$80.50
Technical/User Documentation	20	$35.00	$700.00	$595.00	$805.00
CBC Documentation	500	$35.00	$17,500.00	$14,875.00	$20,125.00
Directory Structure	2	$35.00	$70.00	$59.50	$80.50
Print Support Procedure Manual	30	$35.00	$1,050.00	$892.50	$1,207.50
Problem Log	3	$35.00	$105.00	$89.25	$120.75
Project Planning Documents	8	$35.00	$280.00	$238.00	$322.00
Change Management Request	2	$35.00	$70.00	$59.50	$80.50
Ethernet Log	8	$35.00	$280.00	$238.00	$322.00
Standards Documentation	3	$35.00	$105.00	$89.25	$120.75
Missed Modules List	1	$35.00	$35.00	$29.75	$40.25
Standards Proposal	0.5	$35.00	$17.50	$14.88	$20.13
Session Scripts	3.5	$35.00	$122.50	$104.13	$140.88
Publication Checklist	0.5	$35.00	$17.50	$14.88	$20.13
Lab Documentation	2	$35.00	$70.00	$59.50	$80.50
Handouts	4	$35.00	$140.00	$119.00	$161.00
Training Manual #1	20	$35.00	$700.00	$595.00	$805.00
Training Manual #2	20	$35.00	$700.00	$595.00	$805.00
Address Book	4	$35.00	$140.00	$119.00	$161.00
Personnel Documentation	2	$35.00	$70.00	$59.50	$80.50
Subtotal	1041.5		$36,452.50	$30,984.63	$41,920.38
Benefits @28%:			$10,206.70	$8,675.70	$11,737.71
Subtotal (Salaries + Benefits):			$46,659.20	$39,660.32	$53,658.08
Indirect Cost Rate (52%):			$24,262.78	$20,623.37	$27,902.20
Total Labor Cost (Salaries + Benefits + ICR):			**$70,921.98**	**$60,283.69**	**$81,560.28**
Median Cost +/- 15%			**$70,921.98**	**+/- 10,638.30**	

Equipment Costs

The department purchased a document scanner at the cost of $630 to assist with the data recovery (see Table C-38).

Table C-38

Equipment Purchases	
Scanner	$630.00
Total	**$630.00**

By adding the workers' costs to the recovery and equipment costs, we arrived at a total cost of the incident of $92,500 (see Table C-39).

Table C-39

Total Costs				
Workers' Costs			$20,995.42	+/- $3,149.31
Recovery Items			$70,921.98	+/- 10,638.30
Equipment Purchases			$630.00	
Total			**$92,547.40**	**+/- $13,787.61**
Rounded to Nearest $100.00			**$92,500.00**	**+/- $13,800.00**

The unfortunate aspect about this incident is that the department was going to install a new backup system, which would have greatly reduced the impact of this incident, a week after the server crash occurred. It was simply bad timing that the backup system was not yet installed at the time of the server crash.

Unquantifiable Costs

This incident hangs over this department like a black cloud. No one likes to talk about it, let alone try to remember how many hours were spent working on it. It was a painful event for all employees of the office.

This incident affected its users on two levels. It affected the outside users at a secondary level. Due to the confusion and downtime of the server, the office staff could not conduct their services at the same pace as they could before the incident. The speed and quality of their assistance was lessened by the server failure.

The incident affected the office staff members much more directly. Not only did staff members have to recreate files and try to keep up with work without having backup files to consult, but their trust in the technology was reduced to nothing.

As one incident handler explained, twenty-five years ago, everyone expected hardware to fail simply because it was not very sophisticated. Today, with the more sophisticated equipment available, staff members are not

accustomed to hardware failures anymore and a false sense of security has developed. Consequently, users of the hardware rarely backed up data, depending solely upon the server. Now, every employee is aware of the possibility of data loss and takes extra measures to prevent such an occurrence from happening again.

12. The Linux Crack

The Incident and Its Resolution

A system administrator from a west coast university contacted the network incident investigator at a CIC member institution. A user from an address in the member institution's domain was attempting to gain access to the west coast university's network. The information in the address was insufficient to pinpoint a single user, so the incident investigator traced the Ethernet address back from the network hub to a machine in the central computing center building. The investigator procured permission to access the machine from a colleague of its owner (who was out of town). A cursory scan revealed that the version of Linux on the machine had been exploited using the "phf" bug to gain root access and obtain the password file. Hence, a hacker was using the exploited machine as a jumping point to the west coast university. Once the investigator determined how the hacker gained root access, he pulled the non-production machine from the network.

Further investigation of the infected machine revealed two programs hidden in a ". " directory off root. One appeared to be a denial of service program that engaged other machines to kill them; the other turned out to be a packet sniffer that wrote its output to "tcp.log". When the incident investigator checked, the tcp.log was empty. To determine how severe the damage may have been, he allowed the sniffer to run for a day and checked to see how many network passwords could be stolen. The results were significant enough to warrant having the five people on the network change passwords. Once he assured himself that passwords had been compromised, the incident investigator contacted the campus police department.

To determine where the hacker originated, the incident investigator pulled the network logs and searched the connections. He identified a commercial ISP to whom he sent an e-mail message, hoping that the system administrator could provide additional information on the PPP connections into the compromised machine. He also asked the system administrator at the west coast university to check for similar activity. The system administrator reported that a hacker from the same commercial ISP had indeed attempted to connect to three computers in his network, and further, all three were part of the same group that had been unsuccessfully attacked from the investigator's machine.

Meanwhile, the investigator received a phone call from a department in the university about a hacker who had deleted a number of files on their research servers. The architecture of the network allowed the hacker to enter one machine and move freely among four others. The five servers contained the research of 10 graduate students. After a scan of the departmental machines, the incident investigator determined that the hacker used the same "phf" bug and left traces on the machine similar to earlier activity. A search of the connection logs revealed that this hacker had indeed originated from the same commercial ISP as in the earlier case. Now the hacker had become more than just a nuisance, he or she was deleting files.

Because the hacker's actions had become malicious and illegal, the incident investigator turned his attention to tracking the individual at the commercial ISP. With some cooperation from the commercial ISP, the incident investigator was able to simultaneously implicate a single user in both the original Linux machine and the department attacks.

Costs and Incident Implications

Our analysis revealed that the quantifiable cost of this incident to the university was a minimum of **$2,900**. This figure includes both the workers" costs, mostly borne by the incident investigator and police, and an estimate of the costs of the Chemistry research deletion.

Immediately following the detection of the hacker, the "phf" bug vulnerabilities were patched on the affected networks. According to the incident investigator, preventing this common, yet often overlooked, security hole takes "no more than a couple of minutes." In this isolated case, it may have saved the lost workers' costs and hours of graduate student time, assuming, of course, that this was the only tool available to the hacker. In addition to patching the "phf" hole, all affected machines went through upgrades to establish a generally more secure network.

One of the problems the incident investigator alluded to was the poor reporting of DNS entries on the network. Better reporting might have saved him four hours in the hub tracing the Ethernet address. The incident investigator said that his institution already has a policy of registering the machines prior to connecting them to the network, but that it is followed insufficiently.

Workers' Costs

Our calculations for workers' costs include a measure for benefits and indirect costs. To calculate the costs associated with the staff password change, we estimated the average time required to change passwords and have assumed an average wage rate for the employees involved (see Table C-40).

Table C-40

Workers' Costs					
Title	Hours	Cost/Hr.	Total	-15%	15%
Incident Investigator	43	$15.68	$674.24	$573	$775.38
System Administrator	3.75	$25.00	$93.75	$80	$107.81
Consultant	1	$24.95	$24.95	$21	$28.69
Detective	10	$18.63	$186.30	$158	$214.25
Staff	0.833	$15.00	$12.50	$11	$14.37
Subtotal	58.583		$991.74	$842.97	$1,140.50
Benefits @ 28%			$277.69	$236.03	$319.34
Subtotal (Salary and Benefits)			$1,269.42	$1,079.01	$1,459.83
Indirect Costs			$660.10	$561.08	$759.11
Total Labor Cost			$1,929.52	$1,640.09	$2,218.95
Median Cost +/- 15%				$1,929.52	+/- $289.43

Users' Costs

The majority of the users' costs are in the form of lost research to graduate students. Based on an estimate of the time lost to each of the 10 students and an assumption on the monetary value of their time, we calculated an estimated loss. We have not included a measure for benefits or indirect costs, so this number should be considered a lower bound. Our access to these students was restricted, so we were not able to determine whether

or not they were employed by the university. These assumptions are reasonable in our opinion, yet the figures should not be considered precise (see Table C-41).

Table C-41

Users' Costs					
Number of Users	Hours	Cost/Hr.	Total	-15%	15%
12	80	$12.00	$960.00	$816.00	$1,104.00
Total Users' Cost			$960.00	$816.00	$1,104.00
Median Cost				$960 .00	+/- $144.00

Total Costs

To arrive at the overall cost of the incident, we added the subtotals of the workers' and users' costs. See Table C-42 for details.

Table C-42

Total Costs				
Workers' Costs			$1,929.52	+/- $289.43
Users' Costs			$960.00	+/- $144.00
TOTAL COSTS			$2,889.52	+/-$433.83
Rounded to Nearest $100.00			$2,900.00	+/- $400.00

Other Cost Issues

The only upgrade costs that we have included in our analysis are those associated with the original Linux machine. These upgrades have been included because they were necessary to bring the incident to a close. We have assumed that the other upgrades would have taken place regardless of this incident and therefore should not be included as costs.

Unquantifiable Issues

We were unable to quantify effectively the extent to which the hacker invaded the university networks. We are certain that the same individual attacked the Linux machine and the department, but do not know if he hacked into other areas within the university domain as well. It is possible that he damaged or abused other systems, but we cannot assume that occurred and have no way to cost out the possibility.

13. The Mismanaged Machine

The Incident and Its Resolution

During the spring of 1997 a system administrator received an inordinately large number of compromised computing account complaints from a single department within the university. A cursory glance at some of the machines in the department revealed the tracks of hacker activity. Telltale signs were a directory called "Egg Drop," an IRC bot, and directories named .....

After a more complete examination of the machines, personnel determined that the entire departmental network was compromised. Using "Egg Drop," an IRC server, a hacker had gained access to the network through a machine set up by a graduate student. The hacker installed a sniffer on the network and stole passwords, both internal and external to the university. Estimates of the number of passwords stolen ranged in the hundreds.

Computing security personnel encouraged users to change their passwords and search their home directories for suspicious or otherwise unknown files. Switches were installed and the departmental network was segmented so that the compromised machines were separated from private, lab, or public access machines.

Part of the process of resolving the incident involved completing network upgrades. The scheduling process was rearranged to give priority to the compromised departmental network. The combination of the upgrades and network segmentation re-established the integrity of the system and minimized the potential magnitude of loss for any future incidents.

Costs and Incident Implications

Our analysis reveals a total monetary cost of **$9,300**. This figure includes the workers" costs of resolving the incident and an estimate of the costs of changing passwords.

Workers' Costs

Five university employees in addition to the network design office were involved in resolving the incident. Based on their reported hours and published wage rates, we determined that 190 hours were spent in the resolution at a cost to the university of approximately $7,800 (see Table C-43).

Table C-43

Workers' Costs					
Title	Hours	Cost/Hr.	Total	-15%	15%
Programmer	5	$17.31	$86.54	$73.56	$99.52
Computing Administration	5	$24.52	$122.60	$104.21	$140.99
System Administrator	65	$12.00	$780.00	$663.00	$897.00
Professor	50	$34.62	$1,730.77	$1,471.15	$1,990.38
Programmer	15	$26.44	$396.63	$337.14	$456.13
Network Operations	50	$18.27	$913.46	$776.44	$1,050.48
Subtotal	190		$4,030.00	$3,425.50	$4,634.50
Benefits @ 28%			$1,128.40	$959.14	$1,297.66
Subtotal (Salaries + Benefits)			$5,158.40	$4,384.64	$5,932.16
Indirect Costs			$2,682.37	$2,280.01	$3,084.72
Total Labor Costs			$7,840.77	$6,664.65	$9,016.88
Median Cost +/- 15%				$7,840.77	+/- $1,176.12

Users' Costs

Potentially 150 faculty, staff, and students were required to change their passwords. Our inability to speak with each affected individual constrained us from calculating the most accurate measure of user loss. For the purposes of this incident report, we estimate only the time lost as a result of changing university passwords. We assume an average wage rate for each affected group member and multiply that rate by an estimated amount of time needed to change a password. Our calculations reveal an estimated users' cost of approximately $1,500 (see Table C-44).

Table C-44

User Costs					
Number of Users	Hrs.	Cost/Hr.	Total	-15%	15%
150	37.5	$20.00	$750.00	$637.50	$862.50
Subtotal	37.5		$750.00	$637.50	$862.50
Benefits @28%			$210.00	$178.50	$241.50
Subtotal (Salaries + Benefits)			$960.00	$816.00	$1,104.00
Indirect Cost Rate @ 52%			$499.20	$424.32	$574.08
Total Users' Costs			$1,459.20	$1,240.32	$1,678.08
Median Cost				$1,459.20	+/- $218.88

Total Costs

Total quantifiable costs of the incident are estimated by adding the workers' and users' costs (see Table C-45).

Table C-45

Total Costs				
Workers' Costs			$7,840.77	+/- $1,176.12
Users' Costs			$1,459.20	+/- $218.88
TOTAL COSTS			$9,299.97	+/- $1,395.00
Rounded to the nearest $100			$9,300	+/- $1,400.00

Unquantifiable Issues

Apart from the inconvenience of changing departmental passwords, some users ran into problems changing their external site passwords. The system administrator reported a general feeling of ill-will towards the users from the external site administrators.

Some users had their files erased and/or lost work as a result of the incident. The extent of the damage is unclear; however, any time spent recreating lost data should be included as a real cost to the university.

14. The Missing Donors

The Incident and Its Resolution

A university fundraising office solicits pledges from donors regularly. The office is located in an extremely obscure location and is relatively removed from the rest of the university.

During the week after Spring session ended, a break-in occurred at the office. There was no pledging session the day of the break-in, so the staff left the office at 5:00 p.m. Returning to the office the next day at 7:45 a.m., the staff noticed that the following items were missing:

- Server
- Zenith Computer
- Zenith Monitor
- Canon Color Printer (Bubblejet)
- Backup Tape Drive
- Backup Tapes
- Uninterruptible Power Supply

There was no sign that a break-in occurred. It takes two keys to enter the office at all times, even during the day. The light switch to the office is somewhat concealed. Hence, the switch would be difficult to find in the dark unless the perpetrator knew its location. Also, the only elevator that is accessible to the office is a service elevator, which requires keys. Therefore, it was assumed that the theft was an inside job by someone who had access to multiple sets of keys. One suspect was a service employee of the building, about whom members of the office staff had complained. When this person was confronted with the break-in, he denied it. When authorities tried to contact him again, he could not be found.

There was additional, and more valuable, equipment in the office that was not taken. This equipment included 30 to 40 high-quality PCs, a new laser printer, an almost-new color TV, and a VCR. The only PC that was taken (the Zenith) was old and practically worthless to the office. (In fact, the office did not even bother replacing it after the incident; see Table C-47.) The stolen printer was also old. The perpetrator chose not to take any of the cords and left them lying neatly on the tables where the equipment once was.

The server that was removed was kept in a separate room that looks very unassuming. The doors to the room were closed, and when closed, it appears as if the room is just a small closet. The server was extremely heavy, and the service elevator had to be used to transport it to the ground floor.

As far as any of the staff members knows, none of the information from the server has surfaced thus far.

The campus police were called; they took pictures and passed the case to a detective. The missing equipment was replaced within four weeks.

All locks in the office were changed. The lock on the door that leads to the server is accessible only to the office staff, fire department, and police.

The staff determined that not much more could have been done to improve the physical security of the equipment, other than installing security cameras or placing guards at the door. The department decided that these measures were impractical.

Costs and Incident Implications

Our analysis indicates that this incident cost the university approximately **$156,500**. This figure includes workers' costs, the costs of purchasing new equipment, and the potential pledges that the university lost as a direct result of the theft.

The incident received little publicity and, therefore, did not generate complaints from donors. However, it raises the issue of whether or not donors should be made aware that by giving their Social Security numbers, they may be placing themselves at risk. Given the sensitivity of the data on the file server, better care should have been taken to guarantee its protection by, for example, installing a keycard access system and/or monitors. Though these installations are costly, they are probably less expensive than the total cost of this incident.

Workers' Cost

Twelve employees were involved in the resolution of this incident. Based on the hours reported to us, we multiplied the employee wage rate by the total hours worked for the individual, for a subtotal of $6,000. Table C-46 depicts our findings.

Table C46

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Facilities Mgr.	8.5	16.21	137.79	$117.12	$158.45
Asst. Purchasing Agent	0.75	18.32	13.74	$11.68	$15.80
Detective	35.0	18.21	637.35	$541.75	$732.95
Asst. Mgr. - Fundraising Ofc.	2.5	11.78	29.45	$25.03	$33.87
Secretary - Fundraising Ofc.	9.0	9.00	81.00	$68.85	$93.15
Residence Hall Mgr.	3.0	15.63	46.89	$39.86	$53.92
Director Annual Support	5.0	32.69	163.45	$138.93	$187.97
Operations Admin.	5.0	15.24	76.20	$64.77	$87.63
Assoc. Mgr. - Fundraising Ofc.	9	12.50	112.50	$95.63	$129.38
Risk Manager	1.0	23.25	23.25	$19.76	$26.74
Manager - Fundraising Ofc.	25.0	13.70	342.50	$291.13	$393.88
Development Assoc.	90	15.87	1428.30	$1,214.06	$1,642.55
Subtotal	193.75		$3,092.42	$2,628.55	$3,556.28
Benefits @ 28%			$865.88	$735.99	$995.76
Subtotal (Salaries + Benefits)			$3,958.29	$3,364.55	$4,552.03
Indirect Cost Rate @ 52%			$2,058.31	$1,749.56	$2,367.06
Total Labor Cost			**$6,016.60**	**$5,114.11**	**$6,919.09**
Median Cost +/- 15%			**$6,016.60**	**+/- $902.49**	

Equipment Costs

The fundraising office manager provided us with both the estimated value of the equipment that was stolen and the replacement cost. The office spent less than the estimated value of the equipment because they decided not to replace the outdated computer and monitor (see Table C-47).

Table C-47

Equipment Cost		
Type of Equipment	Estimated Value	Cost of New Equipment
Server	$12,403	$12,659
Zenith Computer	$900	did not replace
Zenith Monitor	$200	did not replace
Canon Color Printer	$475	$337
Back-up Tape Drive	$1,448	$1,500
Back-up Tapes	$348	$460
Uninterruptible Power Supply	$350	$312
Subtotal	$16,124	$15,268

Lost Revenue

The fundraising office manager also supplied us with the amount of the potential pledges that were lost as a result of the missing equipment. These figures are represented in Table C-48.

Table C-48

Potential Pledges Raised between Incident and Equipment Replacement						
Employee	# Contacts/Session	$/Contact	# of Sessions	Total	-15%	15%
Caller 1	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 2	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 3	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 4	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 5	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 6	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 7	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 8	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 9	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Caller 10	26	$20.00	26	$13,520.00	$11,492.00	$15,548.00
Total Potential Pledges				$135,200.00	$114,920.00	$155,480.00
Median Cost +/- 15%				$135,200.00	+/- $20,280.00	

Total Costs

We added the subtotals of the workers' costs, equipment costs, and lost revenue to arrive at the total cost of the incident (see Table C-49).

Table C-49

Total Cost of Incident		
Table 1: Workers' Cost	$6,000.00	+/-$900.00
Table 2: Equipment Cost	$15,268.00	
Table 3: Lost Pledges	$135,200.00	+/- $20,280.00
Total:	**$156,468.00**	**+/- $21,180.00**
Rounded to Nearest $100.00:	**$156,500.00**	**+/- $21,200.00**

Unquantifiable Issues

If a donor discovers that his or her Social Security number was disclosed as a result of the theft of the server, he or she may file suit against the university under privacy law. At the very least, a lawsuit will result in negative press for the university. At the very most, a suit can be extremely costly and damaging. One can imagine that figures from this scenario have the potential to make the earlier reported figures relatively insignificant.

All lost information was backed up on tape. However, the staff was unable to translate the information without the missing server. The backup had to be outsourced for translation, which took a considerable amount of time. This could have been avoided by establishing a backup system that did not rely on the server for translation, which would have reduced some costs. There was also a significant delay in the delivery of the new server, which also held up production and therefore increased costs.

While waiting for the replacement equipment to arrive, the staff members, along with three to four student workers, painted the office. This cost, though unquantifiable, could lower the total cost of the incident for two reasons: a) the painting was an overall benefit to the office; and b) the employees that would normally would have been soliciting pledges were not being paid.

15. The Missing Multimedia

The Incident and Its Resolution

The following equipment was stolen from a career planning office: the system file server, its backup tape, a keyboard, and Packard Bell and Apple desktop systems. The file server contained an online database for student reference, budget files, a desktop publishing system and files, a card catalog, and a database for tracking letters.

The senior systems analyst for the office believes that the thief or thieves were either employed by the office or associated with someone who was. The stolen hardware and accessories all came from a single room and only someone familiar with the layout of the office would know exactly where the expensive equipment was stored. Students, for the most part, would have no knowledge of the computer room.

A renovation project at the building in which the career planning office is housed contributed to the theft. Fire doors and outside entries were often left unlocked to allow construction workers easy movement throughout the building. A new door was installed on the file server room, but the office staff never received a key to allow them to lock it. Thus, for most of the renovation process, the room was insecure.

Fortunately, all information on the file server had paper backup copies. Within four days, the office received a temporary server to run the card catalog and databases. According to the systems analyst, little work was affected in the interim. Most of the work repairing the problem was spent re-entering lost data from the paper backups. The office completed the re-entry over a number of weeks.

Costs and Incident Implications

Our analysis indicates that this incident cost the university a minimum of **$11,700**. This figure includes the wage costs of re-entering lost data as well as the purchase of new hardware. The true cost will also include factors that are unquantifiable, an issue that we will deal with in another section.

The office did not have an established disaster recovery plan and little theft deterrence. As a result of the incident, the server room is locked securely each night and backup tapes are locked in another part of the building.

Workers Costs

The senior systems analyst reported that five people on her full-time staff and a number of work-study students were involved in the data re-entry. Based on the hours reported to us, we multiplied the employee wage rate by the total hours worked for the individual. For work-study students, we used $6.00 as an average hourly wage. Labor costs total $2,700 (see Table C-50).

Table C-50

Workers' Costs					
Title		Hours	Cost/Hr.	-15%	15%
Administrative Assistant		5	$17.78	$75.56	$102.22
Office Secretary		60	$9.98	$509.18	$688.90
Office Supervisor		5	$11.70	$49.73	$67.28
Adminstrative Assistant		10	$18.05	$153.46	$207.62
Senior Systems Analyst		3	$18.26	$46.57	$63.01
Subtotal		83		$834.50	$1,129.03
Benefits				$233.66	$316.13
Subtotal (Salaries + Benefits)				$1,068.16	$1,445.15
Work-Study Students		90	$6.00	$459.00	$621.00
Indirect Costs				$794.12	$1,074.40
Total Labor Costs				$2,321.28	$3,140.55
Median Costs +/- 15%				$2,730.92	+/- $409.64

Equipment Costs

The cost of replacing the stolen hardware was $9,000. The career planning office paid a $1,000 deductible to the Risk Management office, which in turn picked up the remaining $8,000, because of the large deductible the university carries. Because the Risk Management office is part of the university community, the complete $9000 should be counted as a loss (see Table C-51).

Table C-51

New Purchases	
Office Contribution	$1,000.00
Risk Mangement Contribution	$8,000.00
Total Hardware Costs	$9,000.00

Total Costs

The total quantifiable cost of the incident was calculated by adding the workers' and new hardware costs (see Table C-52).

Table C-52

Total Costs		
Workers' Costs	$2,730.92	+/- 409.64
Hardware Costs	$9,000.00	
TOTAL COSTS	$11,730.92	+/-409.64
Rounded to Nearest $100	$11,700	+/- $400.00

Unquantifiable Costs

These factors, individually or together, should be considered real or potential costs. Despite the difficulty in quantifying them, they are nonetheless costly to the university community.

We were unable to address user costs completely. Typically, when a server goes down or files are lost, user costs are significant. In this case, however, all lost information was backed up on paper copies. Thus, all employees, clients, and students were able to access the information they needed, albeit with some inconvenience. It is the inconvenience that we cannot capture in monetary terms.

We also have not quantified losses in efficiency. Until all records are restored to the file server, anyone interested in a file must search for the paper copy and eventually re-file it. If this procedure hampers office operation in any way, a cost must be associated with it.

Some minor unreported time may have been spent by the career planning staff speaking with Risk Management, police, and university administration. Despite repeated requests for detailed reports on logged hours, we were unable to obtain the information we needed to analyze these costs. We are certain that such costs are minor.

Some of the files stored on the file server contained students' names and Social Security numbers. Fortunately for the university, the incident received little publicity and, therefore, did not generate complaints from students. However, it raises the issue of whether or not students should be made aware that their Social Security numbers may be susceptible to malicious or fraudulent use. Given the sensitivity of the data on the file server, it could be argued that better care should have been taken to guarantee its protection.

If a student discovers that his or her Social Security number was disclosed as a result of the theft of the server, he or she may file suit against the university under privacy laws. At the very least, a lawsuit would result in negative publicity; at most, a lawsuit could be extremely costly and damaging to the university. Costs from a lawsuit could make the earlier reported figures relatively insignificant.

16. The Night When the Lights Went Out

The Incident and Its Resolution

A security vendor at a university computing and data center performed an unscheduled fire alarm/panel test. A switch relay was activated during the procedure, which caused all systems at the center to shut down. These systems included a university mainframe, several database servers, communications equipment (telephone and electronic), the floor entry system, and the uninterruptible power supply.

As a result, several mission-critical operations were not available during the three hours that the mainframe was down and the 100 minutes that the servers were offline. These operations included the human resources database, payroll, financial operations, and the software that ran the student dial-in registration. The shutdown affected a potential 4,500 staff members.

Several factors contributed to the incident:

- No protocol for the fire alarm/panel tests had been developed.
- The switch relay should have been pulled before the testing. This action alone would have prevented the power failure.
- No serious problems had occurred in the past; hence, there was no sense of urgency about standardizing the procedure.
- The vendor performed the tests, and university staff believed that they were able to perform the tests competently.

Because the test malfunction shut down virtually all power to the computing and data center, the established disaster recovery plan was not entirely workable. The most problematic issues for the disaster recovery team included the following:

- Automatic Vendor Alerts: The Hitachi, IBM and Xerox systems are programmed to call the factory directly in the event of a failure. The downed communications prevented this from happening.
- Missing or misplaced cell phones: Cell phones to facilitate communications in a power outage were not immediately available in the computing and data center. Once the phones were discovered, the disaster recovery team was unsure of the phone numbers for their cell phones.
- Other communication devices: The centrex phones (designed to run on separate power in case of an emergency) were limited in number and not explicitly identified. Later, it was discovered that the wrong phone number had been assumed for the identified phone.
- Lack of a single person in charge: Given the communications failure, it was difficult to formulate a centralized and hierarchical resolution team. As a result, the process was often chaotic.
- Lack of blueprints: No viable means existed for locating and understanding the shunt breakers that were responsible for much of the power in the computing and data center. Thus, personnel were hampered in their efforts to bring systems back online.

- Lack of proper climate control: As the power went off, the mainframe and servers began to heat up. These machines require chillers to keep them working properly. Fans were moved around the room to keep them cool.

Despite all these problems, the disaster recovery team managed to restore all power and bring systems back online within three hours. Their activities included an exhaustive check of the power status of all systems, confirmation and execution of reset procedures for systems, and switching between internal and external power to expedite the resolution process.

Because much of the data and services provided by the computing and data center were critical for other units within the University, extreme care was taken while powering up to ensure the integrity of the hardware, software, and data. The disaster recovery team consulted with university experts on electricity, communications, hardware, and software before starting reset procedures.

Ultimately, the reset and power-up procedures were successful. All data was apparently saved and no hardware or software problems have been reported subsequently.

Costs and Incident Implications

This incident cost the university **$60,000** to **$120,000**. Included in this figure are the wage costs borne by the disaster recovery team, accrued consultant time, and an estimate of the monetary value of the time lost to users of the system. A majority of the cost of the incident is directly attributable to lost worker productivity. User costs, in this case, were difficult to quantify precisely; hence the cost bounds.

Following the incident, a number of disaster recovery initiatives were implemented. They included the following:

- Review and update of physical security measures (that is, access cards issuance and entry procedures)
- Update of documentation for disaster recovery and maintenance issues with regard to
    - Fire alarm system
    - UPS systems
    - Power up and power down procedures
    - Internal and external communications
    - Maps of wiring and electrical connections
    - Training procedures
    - Police response

This complete examination of the disaster recovery procedures will not necessarily prevent an infrastructure failure, although it reduces the probability significantly. It will, however, enable more efficient and effective coordination of the recovery procedures in the future.

Workers' Costs

Twenty employees from the university's operations, telecommunications, and administrative departments were involved in resolving the incident. These employees logged a reported 31 hours in total resolution time for a total cost of $1,400. See Table C-53 for details.

Table C-53

Workers' Costs						
Title		Hours	Cost/Hr.	Total	-15%	15%
Operations Analyst		5	16.83	$84.13	$71.51	$96.75
Network Support Analyst		3	21.25	$63.75	$54.19	$73.31
Telecom. Analyst		3	21.25	$63.75	$54.19	$73.31
Telecom. Manager		3	27.72	$83.16	$70.68	$95.63
User Services Specialist		3	17.79	$53.37	$45.36	$61.37
Central Computing Director		3	36.96	$110.88	$94.25	$127.51
Business Continuity Specialist		3	23.67	$71.02	$60.36	$81.67
Business Continuity Manager		3	24.56	$73.67	$62.62	$84.72
Production Support Analyst		2	17.78	$35.55	$30.22	$40.89
Administration Manager		3	27.72	$83.16	$70.68	$95.63
Subtotal		31		$722.43	$614.07	$830.80
Benefits				$202.28	$171.94	$232.62
Subtotal (Salary + Benefits)				$924.71	$786.01	$1,063.42
Indirect Costs				$480.85	$408.72	$552.98
Total Workers' Costs				**$1,405.56**	**$1,194.73**	**$1,616.40**
Median Cost					$1,405.57	+/- $210.84

Users' Costs

A potential 4,500 staff members were affected by the infrastructure failure.

During the 180 minutes that the mainframe was down and 110 minutes that various servers were down, staff members were unable to access the human resources databases, payroll, financial operations, and the software that ran the student dial-in registration.

We created a number of reasonable scenarios to account for the monetary value of time lost to employees. Given the impossibility of speaking with every affected user, we estimated an average annual wage cost for the employees ($25,000), and calculated an average per hour salary. We then varied the extent to which they might have been affected. Hence, in the three scenarios, wages are constant, but the hours lost to productivity change. It is unclear how much each employee was affected, but we can assume that it was between no time loss and the entire mainframe down time of 3 hours. See Table C-54 for more information.

Table C-54

Users' Costs						
Potential Users	Hours	Salary	Subtotal	Benefits	Indirect Cost	Total
4500	0	$9.39	$0.00	$0.00	$0.00	$0.00
4500	1	$9.39	$42,255.11	$11,831.43	$6,152.34	$60,238.88
4500	1.5	$9.39	$63,382.66	$17,747.15	$9,228.52	$90,358.32
4500	2	$9.39	$84,510.22	$23,662.86	$12,304.69	$120,477.76
4500	3	$9.39	$126,765.32	$35,494.29	$18,457.03	$180,716.65

Our conversations with those involved in the resolution lead us to believe that the productivity of system users was reduced by approximately half. We also accounted for the opportunity costs of the users doing other things with their time. However, given the uncertainty of this estimate, we reported it as a range of potential costs. We feel that the true figure lies somewhere between these two extremes. The total cost to users of the system is somewhere between $60,000 $120,000.

Total Costs

We calculated the total quantifiable monetary cost of the incident by adding the workers' and users' costs (see Table C-55). However, given the relative insignificance of workers' costs, in terms of overall dollar loss, and to guard against a false precision, we do not explicitly include the $1,400 in workers' costs in the total, they are implicit in the error bound. They should, however, be considered real costs in terms of the overall incident. No costs were associated with new purchases. The total also does not include the time spent evaluating the fire alarm/disaster recovery procedures.

Table C-55

Total Costs		
Workers' Costs	$1,405.56	+/- $210.84
Users' Costs	$60,000-$120,000	
TOTAL COSTS	$60,000-$120,000	

Unquantifiable Issues

An unquantifiable factor of this incident was the downed Voice User systems. The Voice User systems at the university provide students, faculty, and staff with information on class schedules, grades, and financial aid information. Because the system is not essential to everyday activities, and it is unclear how often people use it, we could not reasonably estimate the extent to which people were affected. Despite the difficulty in quantifying that loss, it is a real cost and should be considered an addition to the overall cost.

17. The Overflowing Buffer

The Incident and Its Resolution

During a school vacation break, a university student compromised root on the campus e-mail server cluster (11 AIX machines) using a buffer overflow exploit that is readily available on the Internet. He worked from his home, which is located out-of-state, through an ISP.

After considerable research of system logs and other audit materials, technical support staff identified the student, closed the student's account and other accounts he had illegally introduced into the system, and attempted to clean up the system. Formal complaints were filed with the Dean of Students and with the public safety department, and a notice was sent to the student with interim sanctions described.

Approximately two weeks later, the technical staff detected further evidence of root compromise. They took down the systems for six hours to install emergency operating system (OS) patches and to try to "scrub" the system. Because the student had gained access to the encrypted password file, technical staff ran "crack"' to determine which accounts had easily crackable passwords. Crack uncovered 2,500 vulnerable accounts. Technical staff took the precautionary step of changing those 2,500 passwords. Personnel could not conclusively connect the second attack with the student under investigation, although the timing was suspicious. The second attack came shortly after the close of the first day of his disciplinary hearing.

Technical staff determined that a complete OS rebuild of all systems in the cluster was necessary. The OS rebuild took 48 hours to complete and was performed over a holiday to minimize the impact on customers.

A university disciplinary hearing for the student resulted in his expulsion from the university; criminal investigation is pending.

Costs and Incident Implications

This incident cost the university a minimum of **$56,400**. This figure represents the wage costs that accrued during the resolution of the incident, as well as the costs to faculty, staff, and student users who had to change their vulnerable passwords. What it does not represent is the unquantifiable costs related to the two system outages that lasted for a total of 54 hours. We were unable to quantify these costs, however, these costs have the potential to increase the total cost of the incident considerably. For more information regarding these unquantifiable costs, please see below.

Workers' Costs

Thirteen IT specialists and university executives were involved in the incident resolution. The university gathered the wage costs and compiled them for the project. They had extremely detailed records and accounts of this incident, which made the data gathering for this incident straightforward.

Thirteen employees were involved in resolving this incident. Based on the logged hours and wage rates reported to us, we determined that staff spent 551 hours in the resolution of the incident for a total staff cost of $28,700. See Table C-56 for details.

Table C-56

Workers' Cost						
Title	# of	Total Hours	$/Hr.	Total Wages	-15%	15%
IT System Admin	4	402	$25.03	$10,073.40	$8,562.39	$11,584.41
Comp Science SysAdmin	1	3	$23.00	$69.00	$58.65	$79.35
IT Systems Manager	1	25	$30.00	$750.00	$637.50	$862.50
IT Customer Relations	1	36	$27.00	$972.00	$826.20	$1,117.80
Associate Counsel	1	31	$25.00	$775.00	$658.75	$891.25
Hearing Officer	1	9	$33.00	$297.00	$252.45	$341.55
Public Safety Sergeaant	1	20	$17.00	$340.00	$289.00	$391.00
Provost/Vice Provost	3	25	$60.00	$1,500.00	$1,275.00	$1,725.00
Subtotal:	13	551		$14,776.40	$12,559.94	$16,992.86
Benefits @ 28%:				$4,137.39	$3,516.78	$4,758.00
Subtotal (Salaries + Benefits):				$18,913.79	$16,076.72	$21,750.86
Indirect Cost Rate (52%):				$9,835.17	$8,359.90	$11,310.45
Total Labor Cost:				**$28,748.96**	**$24,436.62**	**$33,061.31**
Median Cost +/- 15%				$28,748.96	+/- $4312.34	

Details regarding the workers' cost include the following:

- IT customer relations staff and Systems Manager spent time handling the media repercussions of the incident.

- IT system administrators have spent considerable time on the legal aspects of the incident, such as preparing materials for the disciplinary hearing, testimony, appeals processes, and probation hearing. One system administrator has been subpoenaed for the criminal case pending in the student's home state.

- IT system administrators have spent considerable time preparing for and performing the system rebuilds.

Users' Costs

As a result of this incident, 2,500 faculty, staff, and students were forced to change their passwords. A manager in staff benefits estimated the average wage rate of the faculty and staff members involved at $35.00 an hour. For the students, a time value of $6.00 per hour was used. The current distribution of accounts on the affected cluster of machines is 26% faculty and staff and 74% students. This translates to 650 affected faculty and staff members and 1,850 affected students.

Each individual spent an average of a half hour in changing passwords. This figure is higher than might be expected because many faculty and staff users needed assistance and several attempts to change their password correctly. In addition, students were required to go to the help desk to get a new password.

We included the benefits and indirect cost rates for the faculty and staff members that were affected by the incident. The details of the cost analysis for the affected faculty and staff members are found in Table C-57.

Table C-57

Fac/Staff Users' Costs (changing passwords)					
# of Faculty/Staff	Hours	Cost/Hr.	Total	-15%	15%
650	325.00	$35.00	$11,375.00	$9,668.75	$13,081.25
Benefits @28%:			$3,185.00	$2,707.25	$3,662.75
Subtotal (Wage Costs + Benefits):			$14,560.00	$12,376.00	$16,744.00
Indirect Cost Rate (52%):			$7,571.20	$6,435.52	$8,706.88
Total Fac/Staff Users' Costs			$22,131.20	$18,811.52	$25,450.88
Median Costs			$22,131.20	+/-$3,319.68	

We did not include the benefits and indirect cost rates for the student users affected by this incident because they are not employees of the university. Information regarding the user costs of student users is in Table C-58.

Table C-58

Student Users' Costs (changing passwords)					
# of Students	Hours	Cost/Hr.	Total	-15%	15%
1850	925.00	$6.00	$5,550.00	$4,717.50	$6,382.50
Total Student Users' Costs			$5,500.00	$4,717.50	$6,382.50
Median Costs			$5,500.00	+/- $832.50	

The total user costs are in Table C-59.

Table C-59

Total Users' Costs				
Fac/Staff Users' Costs			$22,131.20	+/-$3,319.68
Student Users' Costs			$5,500.00	+/- $832.50
Total			$27,631.20	+/-$4,152.18

The total of all costs associated with this incident is in Table C-60.

Table C-60

Total Costs				
Total Labor Cost			$28,748.96	+/- $4312.34
Total Users' Costs			$27,631.20	+/-$4,152.18
TOTAL COST OF INCIDENT			$56,380.16	+/- $8,464.52
Rounded to Nearest $100.00			$56,400.00	+/- $8,500.00

Unquantifiable Costs

System outages of 6 hours and 48 hours occurred (two separate occasions) for approximately 37,000 faculty, staff, and students. The first (6 hour) outage occurred on a Monday evening. The second (48 hour) outage was planned, and occurred over a holiday weekend. We determined that it would be impossible to estimate the costs related to this incident because too many factors concerning the system outage are unknown. First, we have no way of knowing just how many users were inconvenienced by the system outage. However, if this was the only factor, we may have been able to come up with some sort of figure. Second, it was impossible for us to determine how many of those users would have been using the system during the second outage which occurred over a holiday weekend. After taking these two factors into consideration, we decided that it would be best to declare these costs unquantifiable.

However, this decision should not erase the costs altogether. These are real costs to the users-costs which could be enormous and increase the total cost of the incident significantly. This should not be ignored when considering this incident.

Another unquantifiable cost that should be considered is the lack of confidence this incident instilled in the users. Users reported that they felt less confident in central systems because of compromised passwords and related password problems. However, this also raised awareness on campus about the importance of "safe" passwords.

Observations

Consequences

1. The IT staff wanted to know if tighter standards for admission to the university could be considered. The student in question was on parole for hacker activities in his home state when he was admitted to the university. These past activities occurred when he was a high school student.

   The university screens applicants for admission for collegiate misconduct, but does not screen for criminal records. Had the student been suspended from another institution of higher education for his hacking activities, he would have had to document his history as part of the application process.

2. Elimination of login (telnet) access to the mail systems is being considered. However, this would require migration from Pine mail for many users. In addition, some development activity would have to be moved to another, separate UNIX cluster.

3. Separation of student e-mail accounts from staff and faculty accounts is being considered.

4. The incident (and all the publicity it has caused) has raised awareness of computer security issues to the University Administration level. An IT customer relations staff member was asked to speak at a high-level administration meeting about the incident and related computer security issues. There is increased visibility of IT security issues and concerns.

5. Stronger employment screening methods are being considered. (The student in question applied for an IT position after the incident occurred and was nearly hired!)

Prevention

1. If there was more vendor commitment to delivering robust code, there would be less need for customization on site. Customized code complicates upgrades and patch installation, increasing the time and effort required to complete them.

2. Better (cleaner) vendor code, requiring fewer patches.

3. More staff resources dedicated to security.

4. Changes are being made in feeder systems to require more robust passwords. Password checking algorithms were in place on the AIX systems to ensure robust passwords. However, passwords changed via Eudora had not been subjected to the same testing. Students were able to request e-mail accounts from within another system that did not use password cracking. Those insecure passwords were propagated into the e-mail system.

18. The Phony FBI Agent

The Incident and Its Resolution

A student contacted the computer specialist at his university because he received an e-mail from what appeared to be an FBI agent. The FBI agent informed the student that he was a suspect in a child pornography ring and that the FBI would be watching his activity very closely. The student felt a certain amount of anxiety about this information and promptly contacted the computer specialist.

The computer specialist suspected that this was a prank and checked the headers of the e-mail that the student received. It appeared that the e-mail was sent from someone in Singapore. He asked the student if he knew of anyone in Singapore. It turned out that the student had a group of friends living in Singapore who were, indeed, playing a prank. The student decided not to pursue the incident any further, other than asking the computer specialist if he knew any tricks of the trade that could be used in revenge.

The Costs and Its Implication

This incident is what we refer to as an "ankle biter"-that is, it is a relatively small incident that takes little time to solve and does not cost much. Keep in mind, however, that the number of ankle biters a university receives each day can be large. Over the course of a year, these little ankle biters can end up being quite costly.

Total Costs

The total cost of this incident was **$30**. The only costs that are quantifiable in this incident are the workers' costs. One employee spent thirty minutes resolving this incident. The details of the costs can be found in Table C-61.

Table C-61

Workers' Cost					
Name	Hours	Cost/Hr.	Total	-15%	15%
Comp. Specialist	0.5	$31.25	$15.63	$13.28	$17.97
Subtotal:	0.5		$15.63	$13.28	$17.97
Benefits @ 28%:			$4.38	$3.72	$5.03
Subtotal (Salaries + Benefits):			$20.00	$17.00	$23.00
Indirect Cost Rate (52%):			$10.40	$8.84	$11.96
Total Labor Cost			$30.40	$25.84	$34.96
Median Cost +/- 15%			$30.40	+/- $4.56	
Rounded to nearest $1.00			$30.00	+/- $5.00	

Unquantifiable Costs

Psychological costs are a factor in this incident. The student was genuinely worried that the FBI was investigating him for a serious crime. Only when it turned out to be a prank could he relax. Though impossible to quantify, these are real costs that should be considered.

19. The Politics Surrounding the Gopher

The Incident and Its Resolution

During the summer of 1997, a hacker gained root access to a campus-wide information server (a gopher server). The system administrator, who discovered the break-in via a nightly "COPS" report, determined that the hacker gained access by using a dial-in pool from another university that required no authentication. He or she then exploited a vulnerability in the public gopher client running on a server which allowed a shell account. Finally, the hacker used a recently published exploit of the UNIX 'at' command or exploited 'setuid perl' to gain root access and added the account to the password file. Subsequent investigation revealed that the hacker snooped the system for at least four days before the break-in to get a copy of the password file and determine the operating system. The account added to the system attempted to disguise itself as one of 150 ftp-only accounts on the system for Web page management.

A similar root compromise occurred using the public gopher client two years before this incident. At that time, they fixed the client to resolve the problem, but an intervening operating system upgrade apparently re-opened the hole. When the original compromise occurred, IT staff asked that the public client be disabled. However, they were unable to convince the management of the campus computing environment that this step was necessary.

To resolve the situation, the system administrator first disabled the hacker's account, requested that all users on the system change their passwords, and verified that commonly modified programs were still intact. CERT and the university's incident investigator were notified. The investigators quickly decided that it was not worth the time to fix the gopher client and they shut it down permanently. This action did not harm the university community, because a more secure LYNX public client had been available for a year. Therefore, campus users of the gopher client were directed to use the LYNX client; off-campus users were disabled.

The perpetrator could not be traced since the dial-in pool required no authentication; anyone who knew the phone number to the university's system could get into it.

IT staff determined that this break-in did not likely result in any serious or significant changes that required a reload of the operating system. However, they decided to complete a thorough reload of the operating system with the next upgrade. They also decided to update the version of Perl that was being used in order to fix the setuid perl problem.

Costs and Incident Implications

Our analysis indicated that this incident cost the university **$7,600**. We based this figure on the workers' costs to rectify the situation as well as the users' costs related to password changes.

Workers' Costs

Eight employees worked for 190 hours on this incident. Based on the hours reported to us, we multiplied the employee wage rate by the total hours worked for each individual. The total workers' cost for this incident is $7,400. Table C-62 depicts our findings.

Table C-62

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Project Leader Specialist	50	$22.13	$1,106.50	$940.53	$1,272.48
Programmer/Analyst	20	$18.59	$371.80	$316.03	$427.57
Programmer/Analyst	40	$15.13	$605.20	$514.42	$695.98
Technology Specialist	20	$21.90	$438.00	$372.30	$503.70
IT Manager	8	$15.20	$121.60	$103.36	$139.84
IT Security	8	$16.31	$130.48	$110.91	$150.05
Senior Systems Programmer	40	$23.15	$926.00	$787.10	$1,064.90
IS Supervisor	4	$31.94	$127.76	$108.60	$146.92
Subtotal	190		$3,827.34	$3,253.24	$4,401.44
Benefits @ 28%			$1,071.66	$910.91	$1,232.40
Subtotal (Salaries + Benefits)			$4,899.00	$4,164.15	$5,633.84
Indirect Cost Rate @ 52%			$2,547.48	$2,165.36	$2,929.60
Total Labor Cost			**$7,446.47**	**$6,329.50**	**$8,563.44**
Median Cost +/- 15%			**$7,446.47**	**+/-$1,116.97**	

Users' Costs

Fifteen users, all employees of the university, had to change their passwords. It was estimated that the common wage rate was approximately $20.00 an hour and that each user spent fifteen minutes changing his or her password. It is highly possible that more time was spent changing each password, but because there is no way for us to determine the exact amount of time for each user, we decided to err on the side of caution. Results can be found in Table C-63.

Table C-63

Users' Costs					
# of Users	Hrs.	Cost/Hr.	Total	-15%	15%
15	3.75	$20.00	$75.00	$63.75	$86.25
Subtotal	3.75		$75.00	$63.75	$86.25
Benefits @ 28%			$21.00	$17.85	$24.15
Subtotal (Salaries + Benefits)			$96.00	$81.60	$110.40
Indirect Cost Rate @ 52%			$49.92	$42.43	$57.41
Total Users' Cost			**$145.92**	**$124.03**	**$167.81**
Median Cost +/- 15%			**$145.92**	**+/- $21.88**	

Total Costs

The total costs to the university from this incident were calculated by adding the workers' costs and users' costs (see Table C-64).

Table C-64

Total Costs				
Workers' Cost			$7,446.47	+/- $1,116.97
Users' Costs			$145.92	+/- $21.88
TOTAL COSTS			$7,592.39	+/- $1,138.85
Rounded to Nearest $100.00			$7,600.00	+/- $1,100.00

Prevention of Incident

This incident could have been prevented if the public client had been discontinued in January 1995, the time of its first breach. Not having the public client would have eliminated all costs of the incident.

20. The Posted Password

The Incident and Its Resolution

A hacker cracked the password file on a department's UNIX server. The hacker then posted the list of user IDs and passwords on an IRC, allowing several individuals access to hack into system.

The system administrator and the system owner discussed options and constructed the following plan. First, they disabled all user accounts that were accessed. They then forced all users of the server to change their passwords to more secure ones. Next, they increased system security by fixing security holes. Finally, they logged the names and addresses of the ISPs from which the hackers came.

According to the system administrator, no permanent damage seems to have occurred. The increased security measures will inconvenience users slightly. A new tape backup drive that will back up all Windows NT and UNIX computers will be purchased at a later date to handle a more serious incident. This backup drive, however, was going to be purchased eventually and was not a direct cost of this incident. The security upgrades that occurred could have taken place earlier, which might have protected the server from this incident.

Costs and Incident Implications

Our analysis indicated that this incident cost the university **$210**. We based this figure on the workers' costs to rectify the situation and the users' costs to change their passwords.

Workers' Cost

Two employees worked for 4.5 hours to resolve this incident. We multiplied the employee wage rate for each individual by the total reported hours worked. The total workers' cost for this incident is $180. See Table C-65 for details.

Table C-65

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Assoc. Professor	0.5	$38.80	$19.40	$16.49	$22.31
Subtotal:			$19.40	$16.49	$22.31
Benefits @ 28%:			$5.43	$4.62	$6.25
Subtotal (Salaries + Benefits):			$24.83	$21.11	$28.56
Grad. Student Employee	4.0	$12.00	$48.00	$40.80	$55.20
Subtotal			$72.83	$61.91	$83.76
Indirect Cost Rate (52%):			$37.87	$32.19	$43.55
Total Labor Cost			**$183.54**	**$156.01**	**$211.07**
Median Costs +/- 15%			**$183.54**	**+/- $27.53**	

Users' Costs

Five employees needed to change their passwords as a result of the incident. These employees made an average of $18 per hour and spent approximately fifteen minutes each to change their passwords. The user costs accrued while changing passwords are $22.50. (See Table C-66 for details.)

Table C-66

Users' Costs					
# of Staff	Total Hours	Cost/Hr.	Total	-15%	15%
5	1.25	$18.00	$22.50	$19.13	$25.88
Total Users' Costs	**1.25**		**$22.50**	**$19.13**	**$25.88**
Median Costs +/- 15%			**$22.50**	**+/- $3.38**	

Total Costs

To determine total costs, we added the workers' costs to the users' costs to arrive at $210. Details are found in Table C-67.

Table C-67

Total Costs				
Total Labor Costs			$183.54	+/- $27.53
Total Users' Costs			$22.50	+/- $3.38
Total Costs			**$206.04**	**+/- $30.31**
Rounded to nearest $10.00			**$210.00**	**+/- $30.00**

Observations

This small incident has done some good in the department, according to the system administrator. All users became more aware of the security problems that are associated with bad passwords. Also, computer and network security within the department will be handled with greater care as a result of the incident. Both the system administrator and the professor consider themselves lucky that this incident was not as damaging as it could have been.

Even though the incident may have raised awareness, the system administrator states that there is still the false sense of security that is now felt by both himself and the system owner. The system owner describes it as an "electronic violation" which caused him concern.

21. The Spawning

The Incident and Its Resolution

A UNIX system administrator logged into his machine as a superuser and noticed that two unfamiliar processes were launched after login. Immediately suspicious, the system administrator went to edit his *".profile"* and was surprised to find that it did not exist. After executing a command to list all system files, he found that no files existed; they had apparently been erased. The system administrator suspected that a hacker had obtained root access and maliciously modified the system to erase all operating system files.

Within two minutes of discovering the problem, the system administrator examined the *".sh-history"* files for any evidence of tampering with the superuser account directory, saved data that had the potential to be helpful in an investigation, and failed in an attempt to logon on as a non-superuser to analyze the extent of the damage. Fearful that the hacker was online and continuing to corrupt the system, the system administrator brought the entire system down.

Subsequent attempts to log into the system in single user mode failed. It became apparent that the operating system had to be rebuilt from backups. After restoring the operating system, the system administrator successfully logged on in single user mode. He began a search for his account ID in the *".sh_history"* files of all the student directories. The search revealed at least one account that had references to the system administrator's account. His analysis showed that the hacker had logged into a student account and changed to the directory of another account. He or she then issued a command to gain root access on the campus student UNIX machine and sent files belonging to a third student to an external address via e-mail.

Confident that he knew what had happened, the system administrator restored all files from backups and brought the system back online for student use. He had not, however, identified the person responsible for the attack. The system administrator felt that the incident warranted further investigation.

After isolating the account used to gain root access, the system administrator was able to trace the attack to a single student user. The student, an employee of the university, was referred to university counsel, terminated from his position, and his computing privileges suspended. Days later, a friend of the suspected student phoned the system administrator to profess his friend's innocence and took responsibility for the attack.

Costs And Incident Implications

Our analysis reveals that the total quantifiable loss to the university for this incident was between **$18,400** and **$24,400**. This figure includes the wage costs resulting from the incident investigation and resolution, as well as an estimate of users' costs.

The attack on the main student UNIX machine resulted in the loss of student computing services for a potential 1,000 users for three hours. This estimate of 1,000 affected students is based on historical login rates for a period similar to the time the server was down. Students were unable to access their e-mail accounts, login to the server from home, and access their file storage. Faculty were generally not affected because their accounts are run on another server.

Workers' Costs

Six university employees were involved in resolving the incident for a total of 190 hours. Based on these reported hours and wage rates, we calculated workers' costs (see Table C-68).

Table C-68

Workers' Costs					
Title	Hours	Hourly Wage	Total	-15%	15%
System Administrator	100	$21.45	$2,145.05	$1,823.29	$2,466.81
Senior Programmer	5	$32.51	$162.55	$138.17	$186.93
Programmer	5	$31.49	$157.43	$133.82	$181.04
Computing Center Director	2	$56.56	$113.11	$96.15	$130.08
Campus Police	250	$25.00	$6,250.00	$5,312.50	$7,187.50
University Counsel	15	$43.58	$653.73	$555.67	$751.78
Subtotal	377		$9,481.87	$8,059.59	$10,904.15
Benefits			$2,654.92	$2,256.68	$3,053.16
Subtotal (Salaries + Benefits)			$12,136.79	$10,316.27	$13,957.31
Indirect Costs			$6,311.13	$5,364.46	$7,257.80
Total Labor Costs			$18,447.92	$15,680.73	$21,215.11
Median Costs				$18,447.92	+/- $2,767.19

Users' Costs

The estimate for users' costs is based on scenarios which vary depending on the number of productive hours lost to students as a result of the hacker attack. In this incident, the only real loss to students was time; all information was restored from backups. What is uncertain is how much the incident affected each of the potential 1,000 students. Hence, we varied the number of productive hours lost from 0 to 3. Given the short period for which the system was down and the generally nonessential nature of the services rendered inaccessible, we believe that overall loss to users was minimal. We estimate that overall loss to users was within the range of $0.00 to $6,000.00 (see Table C-69).

Table C-69

Users' Costs			
Number of Users	Hours	Cost/Hr.	Total
1000	0	$6.00	$0.00
1000	1	$6.00	$6,000.00
1000	2	$6.00	$12,000.00
1000	3	$6.00	$18,000.00
Estimated User Loss		$0.00 - $6000.00	

Total Costs

The total quantifiable cost to the university is calculated by adding workers' and users' costs (see Table C-70).

Table C-70

Total Costs			
Workers' Cost		$18,447.92	+/- $2,767.19
Users' Cost		$0.00 - $6,000.00	
TOTAL COSTS		$18,447.92 - $24,447.92	+/- $2,767.99
Rounded to the nearest $100		$18,400.00 - $24,400.00	+/- $2,800.00

Other Cost Issues

Charges were leveled against the individual and prosecution proceedings begun. State lawyers, however, are prosecuting the hacker; therefore, their costs have not been included in our cost estimates.

Unquantifiable Issues

One factor that we are unable to quantify is the extent to which the hacker invaded other university networks. It is certainly possible, given the maliciousness of the attack, that the individual damaged other systems as well.

Costs can be attributed to the student who was falsely accused of attacking the server and, therefore, lost his job. It is not clear that the student did not have some part in the incident; nevertheless, real costs are associated with losing his computing privileges and employment.

22. The StatD Overflow

The Incident and Its Resolution

A site external to the university (Site A) notified the central computing center's security officers of an attack originating from a university UNIX cluster. The Site A system administrator sent the log data from the attack to a university network specialist who traced the attack to a compromised account. The account's last login originated from the United Kingdom.

The security officer is unsure how the hacker compromised the account. The security officer did, however, find an .rhost file in a ++ file. The hacker created a "back door" for easy access to the account for anyone who knew that it was compromised. Once the hacker gained access to the account, he or she attempted a StatD overflow attack on site A. The StatD overflow attack allows various users root access to the compromised systems. To resolve the situation, the network specialists locked down the compromised account. The legitimate user was no longer a student at the university; hence, the action created no administrative problems for any users.

Subsequent to the account shut down, the security officers were notified of an attack on another external site (Site B). Again, the logs traced the hack attempt back to the compromised account. The unsuccessful attack, it was discovered, happened before the account lock down. The university made no attempt to track the individual. Given the sophisticated nature of the attacks, and the possibility of further attacks, the security director felt that the best course of action was to deny access to the hacker. The external sites were apprised of the resolution efforts.

Costs And Incident Implications

Based on our calculations this incident cost the university **$100.00**. This figure includes all wage costs attributable to the incident. The figure does not include any costs external to the university; hence, the costs accrued by site A and B were not accounted for. All costs resulting from this incident are attributable to the wage costs of repair, as users were not affected.

To prevent a similar attack in the future, security personnel suggested that the university might set up an automated program to check for .rhost files in ++ directories. Presumably, this procedure would send a signal to system administrators of suspicious activities. The other suggestion was to improve the procedures for closing out inactive accounts. As students leave the university, they are given a six month "grace" period on their accounts. Some students choose to take advantage of this, others do not. It is the inactive accounts that are most problematic because a hacker using one does not have the worry of a legitimate user noticing suspicious activity.

Although the costs of this incident to the university were trivial, it represents a type of incident that occurs frequently and has the potential to occupy a large share of the security personnel's time. Over time, the accumulated costs of these individual incidents could become quite substantial.

Wage Costs of Repair

Four university employees were involved in the incident resolution for a total of two hours. To calculate the university's costs, we multiplied wage rates by the number of reported employee hours. We also included a measure for benefits and indirect costs. The results are shown below in Table C-71.

Table C-71

Workers' Costs					
Title	Hours	Cost/Hr.	Total	-15%	15%
Resident Programmer	1.25	$31.90	$39.88	$33.90	$45.86
Security Director	0.25	$38.86	$9.72	$8.26	$11.17
Incident Response Analyst	0.25	$15.86	$3.96	$3.37	$4.56
Staff Assistant	0.25	$16.75	$4.19	$3.56	$4.81
Subtotal	2		$57.74	$49.08	$66.41
Benefits			$16.17	$13.74	$18.59
Subtotal (Salaries + Benefits)			$73.91	$62.83	$85.00
Indirect Costs			$38.43	$32.67	$44.20
Total Labor Costs			$112.35	$95.49	$129.20
Median Cost +/- 15%			$112.35	+/- $16.86	
Rounded to the Nearest $100.00			$100.00	+/- $20.00	

Total Costs

The total costs of the incident are borne out only by the wage costs of repair. No other costs are associated with the incident; there were no user, incidental or new purchase costs that were applicable.

Unquantifiable Issues

As is the case with all compromised accounts, malicious activity is always a threat. It is not certain how many sites the hacker visited, or for that matter, his or her purpose. If the hacker visited two sites, it is likely that he or she tried others, both internally and externally. However, the security personnel are not certain whether the hacker successfully destroyed or altered any information on university servers. Because of this, we are unable to account the true cost to the university.

A hacker diminishes a university's reputation to the extent that an impression is created among other computing centers that a university's computing environment is insecure. This sort of incident may do little by itself to alter the perception of a university, but a repetition of this sort of event will inevitably hurt a university in the long run, in terms of both monetary loss and diminished reputation.

23. The Stolen Identity

The Incident and Its Resolution

A female student contacted the technology office at her university to report that another individual was using her user ID and sending messages, posing as her, to individuals that she knew. These messages, though not blatant, could have been construed as sexual in nature. They mostly consisted of flirtations directed toward certain male acquaintances. It was highly embarrassing for the student.

The mail was forged in her name and was hard to trace due to a lack of authentication. The computer specialist looked through logs and determined that the messages were being sent from the computer assigned to the lab monitors within one of the computing labs. After conducting an investigation, it was determined that a particular lab monitor was probably sending the messages. The information was sent to the student affairs office for handling. The computing specialist was never notified of the outcome.

Costs and Incident Implications

This incident cost the university approximately **$1,200**. The quantifiable costs consisted entirely of workers' costs.

Workers' Cost

One employee spent 20 hours investigating and resolving the incident. For details, please refer to Table C-72.

Table C-72

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Comp. Specialist	20.0	$31.25	$625.00	$531.25	$718.75
Subtotal:	20.0		$625.00	$531.25	$718.75
Benefits @ 28%:			$175.00	$148.75	$201.25
Subtotal (Salaries + Benefits):			$800.00	$680.00	$920.00
Indirect Cost Rate (52%):			$416.00	$353.60	$478.40
Total Labor Cost			$1,216.00	$1,033.60	$1,398.40
Median Cost +/- 15%			$1,216.00	+/- $182.40	
Rounded to nearest $100.00			$1,200.00	+/- $200.00	

Unquantifiable Costs

We were unable to determine how much time the student affairs office spent dealing with this incident. If there were better communication between the departments within the university, a more complete vision of the total cost of this incident would be available.

Also, psychological costs were borne by the student whose identity was stolen. It is impossible to determine how much this is worth in dollars, but it was an embarrassing situation that affected the student and that should not be ignored. She probably also felt a lack of trust in the system, which is another unquantifiable cost.

24. The Student That Was Threatened to Death

The Incident and Its Resolution

A female student and her boyfriend were at a public computing lab at their university. Both entered a chat room in an IRC and joined the conversation. The boyfriend got into a disagreement with another person participating in the chatroom. The disagreement escalated to the point that the other person threatened that the boyfriend would find his girlfriend's dead body on the steps of the building in which the computing lab was located.

Unfortunately, the police did not record the information needed to track this person while they were investigating the incident. The log monitor appeared not to be aware of any procedures that should be followed if such an incident occurred. By the time the system administrator could investigate, all log information had disappeared.

The system administrator thought that the person may have been in the lab at the same time as the couple, or at least he or she was a current or former student at the same university because the person was familiar with the exact name of the computing lab. The system administrator spent approximately two hours sifting through some other logs to try to determine who else in the lab might have been connected to that Web server. Unfortunately, his efforts were fruitless.

Some guidelines for the lab monitors and help desk staff have been planned, but have not yet been finalized, distributed, or instituted. These policies detail what sorts of information must be collected for various types of incidents and instruct personnel on what to do in various cases. Hopefully, if these policies are followed, incidents such as this one can be resolved with a more definitive conclusion.

Costs and Incident Implications

This incident cost the university **$100**. Although this is not much money, we must consider how much the incident would have cost if the staff had been able to seek out the perpetrator. If it were possible, the individual who sent the death threat would have been pursued and dealt with according to policy. They were unable to do so simply because instructions were not in place to turn to when an incident of this nature occurs. Thus, this serious incident, unfortunately, could not be resolved in the proper manner.

Workers' Costs

Two employees spent three hours investigating this incident. Because it was not possible to pursue the individual who posed the threat, little more could have been done. If proper policies had been in place before the incident, the individual could have possibly been pursued and identified, resulting in more time spent and a higher workers' cost. Refer to Table C-73 for details.

Table C-73

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Sr. Comp. Specialist	2.0	$31.25	$62.50	$53.13	$71.88
Lab Monitor	1.0	$6.50	$6.50	$5.53	$7.48
Subtotal:	3.0		$69.00	$58.65	$79.35
Benefits @ 28%:			$19.32	$16.42	$22.22
Subtotal (Salaries + Benefits):			$88.32	$75.07	$101.57
Indirect Cost Rate (52%):			$45.93	$39.04	$52.82
Total Labor Cost			**$134.25**	**$114.11**	**$154.38**
Median Cost +/- 15%			**$134.25**	**+/- $20.14**	
Rounded to nearest $100.00			**$100.00**	**+/- $20.00**	

Unquantifiable Costs

There were definite psychological costs to the student who was threatened; the fact that it was impossible to determine the identity of the person posing the threats made it even more psychologically threatening. The student had no way of knowing who this person was or how serious he was about the threat. Fortunately, the student was not physically harmed as a result of the incident.

25. The Swedish Bouncer

The Incident and Its Resolution

Two members of the university's technology division received a message from a system administrator at an Australian university that a break-in had occurred in one of their departmental systems. Upon investigation, they discovered numerous telnet connections and failed logins from an ISP in Sweden, and no record of any successful logins.

One member of the technology division ran a program called -"chkwtmp" on the system in question to see if anyone had been covering tracks. He discovered the following three deletions:

- 2 deletion(s) between Wed Dec 31 19:00:00 1969 and Sun Aug 10 9:10:59 1997
- 1 deletion(s) between Wed Aug 20 17:06:32 1997 and Wed Aug 20 17:14:38 1997

He noticed four 'ncb" processes, which took place on Aug 20 at 17:32 and 17:43, right after the above deletion. He did not know what a "ncb' process was, but felt that they looked "suspicious."

He checked the ncbs' environments and found that they were started by "ylmath." Ylmath was either the name of a system in the department or the user name of someone within the department.

He then ran strings on the compromised system (both SunOS and Solaris) and found several of the 'ncb" processes mentioned previously. He realized that the hacker had obtained someone's password from the department to access the system and then used it to get into the system at the university in Australia. The hacker was doing the work, however,-at another machine.

The employee of the technology division sent the above information to his colleague who discovered where the ncb was connected by checking netstat. The ncb was connected at telia.net, an ISP in Sweden. It showed repeated login failures, then successful connections. They discovered that the hacker was logging in as a former graduate student from the department who should have had her account deleted a year earlier.

The employee of the technology division notified the proper authorities and e-mailed the Swedish ISP as well as the system administrator in Australia to inform them of the recent discoveries. They then modified the TCP wrapper configuration on most of the departmental machines, including the system in question, to allow only direct connections from campus networks. Outside access should now be allowed only through the department's login servers. The abused account was deleted.

Costs and Incident Implications

This incident cost the university **$700**. These costs consisted entirely of workers' costs related to investigating and resolving the incident (see Table C-74).

Table C-74

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Sys. Research Prog.	5.0	$19.54	$97.70	$83.05	$112.36
Technologist	9.0	$25.76	$231.84	$197.06	$266.62
User Advocate	2.0	$14.50	$29.00	$24.65	$33.35
Subtotal:	16.0		$358.54	$304.76	$412.32
Benefits @ 28%:			$100.39	$85.33	$115.45
Subtotal (Salaries + Benefits):			$458.93	$390.09	$527.77
Indirect Cost Rate (52%):			$238.64	$202.85	$274.44
Total Labor Cost			$697.58	$592.94	$802.21
Median Cost +/- 15%			$697.58	+/- $104.64	
Rounded to nearest $100.00			$700.00	+/- $100.00	

System administrators described the incident as an embarrassment. The compromised machine was one of the last machines in the department running SunOS, which was not being actively maintained (that is, patched). They were not able to upgrade the machine to Solaris because it was providing AFS services to department Macintoshes via netatalk. As far as the system administrator knew, netatalk was still not working with AFS under Solaris at the time of the incident.

As noted above, the account that was cracked belonged to a former graduate student and should have been deleted a year earlier. The system administration staff in the department was relatively new to the environment at the time of the incident. In addition, the department is one of the larger and more complex departmental systems in its college, if not on campus. The department was in a state of transition. It had completed a major AFS upgrade just before losing its system manager of three years in late spring 1997. It was now in the middle of a push to get all its UNIX systems upgraded to Solaris in order to have its new HP-UX systems functioning in a new lab in the fall and to implement a professor's new Web quiz machine essential to some fall classes. The hacker(s) had good timing, catching the department right: before fall semester and attacking a machine that could not be as secure as most because it was providing essential services.

26. The Swiped Buying Card

The Incident and Its Resolution

One of the participating CIC universities issues a credit card to departmental purchasers for transactions that once required petty cash. The card is in the employee's name and the employee receives monthly statements, but the university is responsible for the monthly balances on purchases. There is a per-transaction constraint on purchases as well as the more typical cap on total purchases.

On March 26 or 27, 1997, an employee received her monthly statement and noticed four charges to a large software company on the last day of the billing cycle, March 24. Certain that she had not made the charges, the employee reviewed her records and called the customer service department at the software company. The employee learned that someone had used her name, university address, and a bogus phone number to order software over the Internet. Once given clearance to obtain software from the company, the perpetrators proceeded to download approximately $500 worth of Macintosh software.

Investigators uncovered a number of facts that led them to believe that the thief was familiar with the credit card account. The perpetrator charged right at the $500 limit; therefore, he or she must have known that the card becomes invalid if the user attempts to make a purchase for an amount larger than the per-transaction fee. In addition, the weekend that the charges were made, the employee had the card on her person; therefore, the card information must have been taken at an earlier date. The employee claimed that she often left the card locked in her desk.

The software company agreed to credit the fraudulent charges. University administrators responsible for the card were informed of the incident and decided not to issue a new card. They reasoned that the number is hardly confidential due to the large number of hands the monthly statement passes through. The public safety unit at the university never apprehended the thief.

Costs and Incident Implications

Our analysis of the incident reveals a total cost to the university of **$120**. This figure includes all workers' costs associated with resolving the incident. No user costs or new purchases occurred in this incident. Because the fraudulent purchases were credited by the software company, no additional money was lost as a result of the unauthorized downloaded software. Despite the small cost figure attached to this incident, a much larger loss is not inconceivable.

The office responsible for issuing the card never relayed a sufficient reason for not destroying the card in question. It appears that the university has done little to deter similar incidents in the future.

The employee now keeps the card in her wallet at all times. Charge receipts are immediately locked up as some of them contain the card number. In addition, the employee contacted her regular vendors to alert them to the unauthorized use of the card.

Workers' Costs

Four university employees were involved in resolving the incident for a total of 4 hours. They included employees from campus police, accounting, communications, and a research institute. Workers' costs were calculated using real wage data and reported logged hours (see Table C-75).

Table C-75

Workers' Costs					
Title	Hours	Cost/Hr.	Total	-15%	15%
Administrative Asst.	2	$13.12	$26.23	$22.30	$30.17
Campus Police	1	$19.35	$19.35	$16.45	$22.25
Communications Staff	0.5	$12.00	$6.00	$5.10	$6.90
Accounting Staff	0.5	$19.50	$9.75	$8.29	$11.21
Subtotal	4		$61.33	52.133475	$70.53
Benefits			$17.17	$14.60	$19.75
Subtotal (Salaries + Benefits)			$78.51	$66.73	$90.28
Indirect Costs			$40.82	$34.70	$46.95
Total Labor Costs			$119.33	$101.43	$137.23
Median Cost				$119.33	+/- $17.90

Other Costs

The fraudulently charged software cost $500. The software company, however, agreed to credit the fraudulent charges. Therefore, the only costs associated with the incident are the workers' costs.

Total Costs

The total costs to the university from this incident are calculated by adding workers' costs and other costs (see Table C-76).

Table C-76

Total Costs				
Workers' Costs			$119.33	+/- $17.90
Cost of Thefts				$500.00
Credits				($500.00)
TOTAL COSTS			$119.33	+/- $17.90
Rounded to Nearest $100.00			$120.00	+/- $20.00

Unquantifiable Issues

The anonymity of downloading software raises unique issues in this type of information technology crime. This software company, for example, was unable to check the IP address that was used to download the software. It

would be in the best interest of all parties to use a more secure authentication procedure. If the thief is savvy enough, however, there is virtually no way to trace the order to a particular person or machine.

The most worrisome problem for the university is the security of the credit card numbers. If the numbers can be taken and the accounts are not changed, the university exposes itself to continued loss, especially of the type of incident analyzed here. Specific guidelines for card security and confidentiality should be established.

If the downloaded software is distributed illegally using the university networks, there is potential for copyright violation lawsuits as well. Fortunately, it appears that this was an isolated incident.

27. The Telnet Demon

The Incident and Its Resolution

The system administrator at an information technology unit discovered three undelivered e-mail messages in the root directory of the server she maintains. It appeared that the messages had been there for a period of months. Subsequent investigation revealed that a hacker had created a new file within the root directory and placed a "telnet demon," or Ethernet sniffer, capable of storing UNIX passwords and IDs. The file contained a large number of staff II)s and passwords. The server that had been compromised was used as the office's domain name and e-mail server.

The absence of a disaster recovery protocol left the system administrator struggling to develop a plan to resolve the problem. She wanted the assistance of the information technology center's technicians, but was unsure of whom to contact. Meanwhile, she was concerned about the openness of her system and about telling the wrong people that there had been a break-in. After three or four calls, she was able to speak with a systems research programmer who advised her to make a clean wipe of the whole system and reinstall the software from scratch. He also advised her on the correct way to shut out the Ethernet sniffer.

After consulting with other technicians, the system administrator developed a plan for resolving the situation. First, the office obtained another UNIX machine to use as a temporary server while the system administrator rebuilt the compromised machine. At the end of the process, she would swap the two machines. Second, all employees affected by the Ethernet sniffer were required to change their passwords when the temporary server went up and again when the swap was made with the clean machine.

The recovery plan was not without its problems. The system administrator was much more experienced with Macintosh machines than with UNIX and this procedure was her first experience in rebuilding a UNIX system. She also had difficulty obtaining the temporary UNIX machine, feeling like the only way she was able to secure the machine was through a "friends network," not through any established information technology channels. Because of the relative inexperience of the system administrator and the tedious nature of the rebuilding process, others in the office felt that she was being too careful during rebuilding and was prolonging the process.

Costs and Incident Implications

Our analysis showed that this incident cost the university **$7,100**. This figure includes workers' costs for repair staff and consultants and time lost as a result of having to change employee passwords. This figure accounts for all quantifiable issues related to the incident, and thus should be viewed as a true lower bound on total costs.

Workers' Costs

The system administrator kept detailed records on logged hours for resolving the situation. Based on these figures and university salary information, we multiplied wage rates for consultants and the repair team by number of hours involved. Our total for the wage costs for repairs is $6,600 (see Table C-77).

Table C-77

Workers' Costs					
Title	**Hours**	**Cost/Hr.**	**Total**	**-15%**	**15%**
System Administrator	127.5	$18.61	$2,372.27	$2,016.43	2728.10475
Technician	30	$19.11	$573.21	$487.23	659.1915
Technician	8	$24.11	$192.90	$163.97	221.8396
Technician	3	$15.00	$45.00	$38.25	51.75
IT Ombudsman	1	$22.04	$22.04	$18.73	25.344275
IT Ombudsman	1	$18.04	$18.04	$15.33	20.743125
Technician	7	$24.07	$168.52	$143.24	193.7957
Subtotal	$177.50		$3,391.97	$2,883.18	$3,900.77
Benefits			$949.75	$807.29	$1,092.22
Subtotal (Salaries + Benefits)			$4,341.73	$3,690.47	$4,992.98
Indirect Cost Rate			$2,257.70	$1,919.04	$2,596.35
Total Labor Costs			$6,599.42	$5,609.51	$7,589.34
Median Cost				**$6,599.42**	**+/- $989.92**

Users' Costs

Twenty-four employees changed their passwords during the rebuilding process. Of these 24, 22 changed them twice, while two employees were employed for only the first round of changes. For some, this meant changing 5 or 6 different passwords. We make the assumption that it takes an employee fifteen minutes to change all of his or her passwords. Given our assumption, we multiplied the employee's wage rate by the amount of time spent altering passwords. The resulting figure for all employees is $500 (see Table C-78).

Table C-78

Changing Passwords	Hours	Cost/Hr.	Total	-15%	15%
Office Staff	0.50	$61.76	$30.88	$26.25	$35.51
Office Staff	0.50	$21.39	$10.70	$9.09	$12.30
Office Staff	0.25	$15.50	$3.88	$3.29	$4.46
Office Staff	0.50	$37.76	$18.88	$16.05	$21.71
Office Staff	0.50	$16.34	$8.17	$6.94	$9.39
Office Staff	0.25	$11.19	$2.80	$2.38	$3.22
Office Staff	0.50	$17.69	$8.85	$7.52	$10.17
Office Staff	0.50	$17.69	$8.85	$7.52	$10.17
Office Staff	0.50	$18.45	$9.23	$7.84	$10.61
Office Staff	0.50	$20.68	$10.34	$8.79	$11.89
Office Staff	0.50	$20.69	$10.34	$8.79	$11.90
Office Staff	0.50	$19.11	$9.55	$8.12	$10.99
Office Staff	0.50	$13.50	$6.75	$5.74	$7.76
Office Staff	0.50	$12.00	$6.00	$5.10	$6.90
Office Staff	0.50	$18.15	$9.07	$7.71	$10.44
Office Staff	0.50	$22.56	$11.28	$9.59	$12.97
Office Staff	0.50	$18.61	$9.30	$7.91	$10.70
Office Staff	0.50	$13.06	$6.53	$5.55	$7.51
Office Staff	0.50	$18.49	$9.25	$7.86	$10.63
Office Staff	0.50	$25.00	$12.50	$10.63	$14.38
Office Staff	0.50	$18.77	$9.38	$7.98	$10.79
Office Staff	0.50	$18.26	$9.13	$7.76	$10.50
Office Staff	0.50	$14.74	$7.37	$6.26	$8.47
Office Staff	0.50	$19.19	$9.59	$8.16	$11.03
Subtotal	11.50		$238.62	$202.82	$274.41
Benefits			$66.81	$56.79	$76.83
Subtotal (Salaries + Benefits)			$305.43	$259.61	$351.24
Indirect Cost Rate			$158.82	$135.00	$182.65
Total Users' Costs			$464.25	$394.61	$533.89
Median Costs				**$464.25**	**+/-$69.64**

Total Costs

The total monetary cost of the incident to the university is calculated by adding workers' and users' costs (see C-79).

Table C-79

Total Costs				
Workers' Costs			$6,599.42	+/- $989.92
Users' Costs			$464.25	+/-$69.64
TOTAL COSTS			**$7,063.67**	**+/- $1,059.56**
Rounded to Nearest $100.00			**$7,100.00**	**+/- $1,100.00**

Unquantifiable Issues

It is still not certain whether the stolen passwords were used for any malicious purpose. If they were, the potential for WAREZ sites and forged e-mail increases dramatically, and with it, university liability for a security lapse, disclosed personal information, copyright violations, and hacking behavior. This is a real cost threat to the university.

An issue that is not captured in our analysis is the personal cost to employees in the form of stress, aggravation, and long hours. The system administrator worked nearly half of her logged hours on evenings and weekends. How this translates into dollar figures is unclear, yet these issues are a real cost to employees.

Observations

The system administrator was disappointed in the response she received from the university technology technicians. When she realized that passwords were being sniffed she was extremely fearful of the implications it held for the security of the entire university network. However, she got the feeling from the people she spoke with that it was of little consequence. Moreover, she still feels vulnerable to hackers because she believes that the university network is not consistently secure.

The office is much more diligent about keeping current tapes than it was before the incident. If the office had had a backup of the original system, the system administrator could have just compared the original and compromised systems and reconciled any differences.

28. The Unauthenticated Satellite

The Incident and its Resolution

This report summarizes a series of IT-related incidents at a university satellite school. The descriptive section of this summary is separated into two parts. Each tells distinct threads of the story of this incident's events. Although this incident is comprised of a number of smaller incidents, we believe that it is appropriate to treat it comprehensively because they all originated from a single user. Moreover, breaking down each individual part proved to be too difficult for estimating costs.

Part A

An executive at a university satellite school received a letter in the U.S. mail that documented the names, Social Security numbers, network user identifications, and default passwords for all incoming first year students whose last names began with the letter "'A." The note was signed fictitiously and suggested that the school "take better care of Social Security numbers." Given the sensitivity of the information, the executive forwarded the letter to the appropriate computer security personnel and executives at the school's main campus.

The computer security personnel determined that such a list did not exist in the form in which it was presented. Therefore, their initial action was to examine the means for obtaining the information and consolidating it in one place. After a brief investigation, they concluded that the information could have been consolidated from a campus computer lab's help desk, but only at the particular satellite school. Given that the list only contained information on that university's students, the director of computer security ended any speculation that information on any other school's students had been compromised. The personal information files were removed from the help desk computer at the request of computer security personnel.

To counteract the potential problems of compromised accounts, security personnel ran a check on network user IDs and passwords to determine the number of students whose accounts might be compromised. A significant number of student ID accounts fell into this category. First-year students still using default passwords were asked to change them to reduce the risk of hacker activity. Computer security personnel believed that the security problem had been taken care of, but they were disappointed that the individual responsible for consolidating the information was never identified.

Part B

Occurring concurrently with the theft of personal information were a number of IT-related incidents, including hacking and mail bombs (to a recipient list twelve pages long) originating from an unauthenticated campus computing site. The mail bomb recipient list was very similar to an already existing legitimate list used for an academic department. By comparing the legitimate and mail bomb list, a computer security employee found that one person who should have been receiving the mail had been removed from the list. This discovery raised suspicions among computer security personnel. They believed that they had a suspect.

Upon this discovery, the computer security center asked employees in the campus computing site familiar with the individual to contact the security director when he entered the lab and relay information on which computer he was using. Through this process, the director logged and monitored his activities over a couple of weeks. The procedure was difficult because the individual frequently moved from computer to computer. However, during one session, the security director was monitoring the individual as he accessed the e-mail account of a first year student whose last name began with A. This piece of information provided a link between the two distinct and previously believed to be unrelated, incidents. The computer security center, however, believed that they needed

more time to gather information before they could prove the individual's guilt. Campus police were apprised of the situation.

Later that month, a student notified officials at the computing center that her computing account had been compromised, and the hacker had disenrolled her from school. Security personnel were aware that their suspect knew the individual and at one point had been reading her e-mail. They also believed that he had access to her Social Security number. The female student was assured that she would be immediately reinstated.

Given this last bit of information, the computing center believed they had enough information to apprehend the suspect. Campus police were dispatched to question the individual the next time he approached the campus computing site. When questioned by police, the student immediately admitted to being responsible for the mail bombs, theft of personal information from the help desk, and disenrolling the student. His account was quickly locked down; he was physically banned from the lab and referred to judicial affairs. Ultimately, the student was allowed to finish the term and then dismissed.

Costs and Incident Implications

Our analysis of these events revealed a total quantifiable cost to the university of **$31,400**. Of this figure, the majority results from workers' costs attributable to resolving the incident. The figure also includes an estimate of the costs to students for changing their vulnerable passwords. Fortunately for most users, this series of incidents did not result in any significant time or information loss. Several unquantifiable cost factors are included in our analysis as well. We deal with those issues separately later in the report.

As a result of the events, personal student information is no longer available at the help desk computers. The university understands the sensitivity of the information and has taken steps to ensure that it is held closely.

One of the main lessons of these events is the potential problem created by unauthenticated machines. Presumably, much of this incident could have been prevented had the individual been required to authenticate to campus computers or the university network. The process of requiring authentication at that lab was already planned before these events took place, but it wasn't in place in time.

Workers' Costs

The magnitude of this series of incidents, coupled with the sensitivity of the information involved, meant that a large group of IT specialists and university executives were involved in resolving the incident. Given this large collaborative effort, we gathered most of our data through the security director because it was logistically impossible for us to speak with everyone involved. What we gave up in precision, we made up for in breadth of coverage. Our calculations for wage costs result from multiplying hourly wage rates and reported hours and then adding a measure for benefits and indirect costs (see Table C-80).

Table C-80

Workers's Costs					
Title	Hours	Cost/Hr.	Total	-15%	15%
Security Director	136	$38.86	$5,285.23	$4,492.45	$6,078.02
Satellite Executive Officer	4	$55.00	$220.00	$187.00	$253.00
Director of Academic Com	5	$55.00	$275.00	$233.75	$316.25
Campus Network (satell)	64	$11.17	$715.01	$607.76	$822.26
Information Specialist	16	$22.42	$358.66	$304.86	$412.45
Residential Programmer	80	$31.90	$2,552.16	$2,169.34	$2,934.98
Systems Engineer II	48	$26.84	$1,288.37	$1,095.11	$1,481.62
Police	64	$15.11	$967.30	$822.20	$1,112.39
Ass. Dir Judicial Affairs	16	$25.05	$400.80	$340.68	$460.92
Incident Response Analyst	64	$15.86	$1,014.91	$862.68	$1,167.15
Research Assistant	32	$17.68	$565.82	$480.95	$650.70
Research Assistant	16	$17.68	$282.91	$240.48	$325.35
Sr. IT Administrator II	4	$46.89	$187.55	$159.42	$215.68
Sr. IT Administrator II	3	$46.89	$140.66	$119.56	$161.76
Sr. IT Administrator	2	$46.89	$93.77	$79.71	$107.84
Administraive Security	1	$22.86	$22.86	$19.43	$26.29
Staff Assistant	6	$16.75	$100.48	$85.40	$115.55
Accounts Mgr	4	$31.90	$127.61	$108.47	$146.75
Subtotal	565		$14,599.10	$12,409.23	$16,788.96
Benefits @28%			$4,087.75	$3,474.58	$4,700.91
Subtotal (Staff Salaries + Benefits)			$18,686.84	$15,883.82	$21,489.87
Lab Assistants	56	6.000	$336.00	$285.60	$386.40
Indirect Cost Rate			$9,891.88	$8,408.10	$11,375.66
Total Labor Costs	**621**		**$28,914.72**	**$24,577.51**	**$33,251.93**
Median Cost				**$28,914.72**	**+/-$4413.82**

Users' Costs

To prevent new or further privacy intrusion, 900 first-year students with vulnerable (that is, default) passwords were required to change them. To calculate a monetary value for their time, we assumed an average time loss for changing a password plus a rate for the value of an average undergraduate's time (see Table C-81).

Table C-81

Users' Costs					
Number of Users	Hours	Cost/Hr.	Total	-15%	15%
900	225	$6.00	$1,350.00	$1,147.50	$1,552.50
Median Cost				$1,350.00	+/-$202.50

Total Costs

The total costs result from adding the workers" and users' costs (see Table C-82).

Table C-82

Total Costs				
Workers' Costs			$30,000.00	+/-$4400.00
Users' Costs			$1,400.00	+/-$200.00
TOTAL COSTS			$31,400.00	+/- $4600.00

Other Cost Factors

For the purpose of this analysis, we have not included any potential or real costs associated with upgrading the campus computing environment to require user authentication. Because the upgrade is not directly attributable to these events, the associated costs are outside this analysis.

Unquantifiable Issues

- *Cost to students due to the invasion of their privacy.* There is a real cost to students whose personal information (user identification, password, Social Security number) was stolen or who were victims of the hacker's invasion of personal e-mail and/or file storage.

- *The effect of the mail bombs on server traffic and speed in mail delivery.* Without extremely complicated system dynamic models, calculating this cost is impossible.

- *The true loss to employees.* It is impossible to capture the true loss to employees simply via wage rates. The costs of stress, aggravation, and frustration resulting from this incident are simply incalculable.

29. The Unidentified Hacker

The Incident and Its Resolution

A system administrator was notified that an individual had hacked into her department's system and acquired root access. The attacker had altered the system's process statistics program and some files in the system administrator's home directory.

Two options were presented to the department to correct the problem:

(1) Since the department's system is attached to the Internet, the site could be shut down because it was contaminated. However, this action would alert the attacker, who would then probably disappear, eliminating the chance of capture.

(2) The site could be left open in order to catch the attacker, which would protect the reputation of the department as well as avoid scaring the users of the system. However, this action would allow the hacker to continue attacking the system with anonymity.

After careful consideration, option (2) was chosen.

The hacker was never identified, but the probable approach used by the hacker was. The operating system used by the department was outdated. Older SunOS(s) and SGI(s) have many patches to keep them secure, but these particular machines did not have many of the patches. Therefore, the machines were vulnerable.

The hacker used a sniffer on the machine and probably ran a Trojan horse as well. As a result, all passwords within the department were compromised. Higher approval within the department was needed to continue attempting to track the individual. This approval was granted two days after it was requested. The IT department provided a newer Sun system with a 4 gigabyte hard drive so that the significant data could be logged. Two weeks later, after hours of monitoring the system, it was reported that no unusual activity had occurred.

Since the perpetrator had not been identified, and two months had passed since notification of the incident, it was determined that two university technology consultants would be employed to shut everything down and start over. The rate of recovering the network was slow and for the most part unproductive.

The operating systems on all the research network machines were reloaded. Additionally, updated system patches were also installed to increase the level of security. The consultants completed this activity.

Costs and Incident Implications

At a minimum, this incident cost the university **$12,600**.

This department did not have an established disaster recovery plan and little theft deterrence. Furthermore, the system that was primarily attacked was outdated and incapable of withstanding an attack. The end result was that the operating systems were reloaded on all research network machines and updated system patches were installed.

The information on the system was not considered sensitive by the head supervisor of the department-the system contained research information and no administrative information. Nevertheless, the information was valuable to the department, and any break-in to the system is considered a threat.

Workers' Costs

Eighteen university employees were involved in resolving the incident. Based on the self-reported log of hours and wage rates taken from university salary publications, it was determined that 463.95 hours were spent in the resolution at a cost to the university of $12,600.

Due to the fact that there were two distinct segments of this incident-the investigation and the resolution-we chose to cost analyze these segments separately, and then total the costs at the end.

Investigation

Sixteen employees were involved in the investigation of this incident. The investigation required approximately 192 person-hours and cost the university $7,000. Detailed figures regarding the investigation of this incident can be found in Table C-83.

Table C-83

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Technologist	10	14.33	$143.30	$121.81	$164.80
Professor	1	44.65	$44.65	$37.95	$51.35
Manager - Sys. Group	17.5	21.72	$380.10	$323.09	$437.12
SysAdmin	43.2	12.94	$559.01	$475.16	$642.86
Technologist	1	15.49	$15.49	$13.17	$17.81
Technologist	3	24.78	$74.34	$63.19	$85.49
Comp. Sys. Specialist	1	11.61	$11.61	$9.87	$13.35
Police Sargeant	1	21.87	$21.87	$18.59	$25.15
Comp. Sec. Consultant	39.75	11.90	$473.03	$402.07	$543.98
Asst. to Vice Provost	2.5	31.20	$78.00	$66.30	$89.70
Sysadmin	57.5	15.95	$917.13	$779.56	$1,054.69
Dir. Residential Comp.	1	19.84	$19.84	$16.86	$22.82
Grad. Research Asst.	2.5	14.01	$35.03	$29.77	$40.28
Security Admin	0.5	8.65	$4.33	$3.68	$4.97
Technologist	3	30.05	$90.15	$76.63	$103.67
Risk Mgmt. Admin.	8	16.64	$133.12	$113.15	$153.09
Subtotal:	192.45		$3,000.98	$2,550.83	$3,451.12
Benefits @ 28%:			$840.28	$714.23	$966.31
Subtotal (Salaries + Benefits)			$3,841.26	$3,265.06	$4,417.44
Consulting Services:					
Two technical consultants of the university were also employed on this project.					
There are two different rates for the university v. department for these two employees.					
For the purposes of this cost analysis, we are using their hourly university wage,					
rather than their consulting wage, to determine the cost of their services.					
Consultant	10	14.33	$143.30	$121.81	$164.80
Consultant	49	12.94	$634.06	$538.95	$729.17
Subtotal:	**59**		**$777.36**	**$660.76**	**$893.96**
Total of Workers' Cost + Consultants:			$4,618.62	$3,925.82	$5,311.40
Indirect Cost Rate (52%):			$2,401.68	$2,041.43	$2,761.93
Total Labor Cost			**$7,020.30**	**$5,967.25**	**$8,073.33**
Median Cost +/-15%			**$7,020.30**	**+/- $1,053.04**	

Resolution

Eight employees were involved in the resolution of this incident: the six who were involved with the investigation, and two were brought in fresh at this stage (Employees 17 and 18). The recovery took less time and cost less than the investigation, but not much less. The cost of resolving this incident was $5,600.

Detailed figures regarding the investigation of this incident can be found in Table C-84.

Table C-84

Workers' Cost					
Title	Hours	Cost/Hr.	Total	-15%	15%
Technologist	8	$14.33	$114.64	$97.44	$131.84
SysAdmin	43.5	$12.94	$562.89	$478.46	$647.32
Technologist	3	$24.78	$74.34	$63.19	$85.49
Comp. Sec. Consultant	21.5	$11.90	$255.85	$217.47	$294.23
Sysadmin	67.5	$15.95	$1,076.63	$915.13	$1,238.12
Security Admin	7	$16.64	$116.48	$99.01	$133.95
Technologist	0.5	$25.24	$12.62	$10.73	$14.51
Risk Mgmt. Admin.	5	$16.54	$82.70	$70.30	$95.11
Subtotal:	156		$2,296.15	$1,951.72	$2,640.57
Benefits @ 28%:			$642.92	$546.48	$739.36
Subtotal (Salaries + Benefits)			$2,939.07	$2,498.21	$3,379.93
Consulting Services:					
Two technical consultants of the university were also employed on this project.					
There are two different rates for theuniversity v. department for these two employees.					
For the purposes of this cost analysis, we are using their hourly university wage,					
rather than their consulting wage, to determine the cost of their services.					
Consultant	16	$14.33	$229.28	$194.89	$263.67
Consultant	40.5	$12.94	$524.07	$445.46	$602.68
Subtotal:	56.5		$753.35	$640.35	$866.35
Total of Workers' Cost + Consultants:			$3,692.42	$3,138.55	$4,246.28
Indirect Cost Rate (52%):			$1,920.06	$1,632.05	$2,208.06
Recovery Costs			**$5,612.47**	**$4,770.60**	**$6,454.34**
Median Cost +/- 15%			**$5,612.47**	**+/- $841.87**	

Investigation and Recovery Total

To arrive at the overall cost of the incident, we added the subtotals of the investigation and recovery segments. See Table C-85 for details.

Table C-85

Overall Cost:				
Investigation Subtotal:			$7,020.30	+/- $1,053.04
Recovery Subtotal:			$5,612.47	+/- $841.87
Overall Cost:			$12,632.77	+/- $1,894.91
Rounded to Nearest $100.00			$12,600.00	+/- $1,900.00

Users' Costs

For two weeks, all users who had permission to use the affected server had problems accessing it. We had difficulty isolating the individual affected users to estimate their overall loss. However, given that, most of the researchers had personal backups of the their work, we believe that the loss of time, and hence the costs, were minimal.

30. The Upgrade Disaster

The Incident and its Resolution

During the last week of March 1997, a school's system administrator performed a software upgrade for the network server that stores student files, financial information, and the school's Web page. The upgrade consisted of updating the portion of the system that serves files to Macintosh computers. Software consultants advised the system administrator to back up all files to tape, delete the directories predetermined for upgrade, install the new software, and finally restore the backed up data to the file server. Although the procedure is time consuming, it is not considered complicated.

Following the backup procedure, the server began crashing. For two weeks, it crashed 10 to 15 times per day. The system administrator consulted with university colleagues and software companies to ascertain the origin of the problem. Near the end of the second week, he discovered that the backup software used to restore the data wasn't fully up-to-date and had restored the data to the Novell server in a corrupted state. Therefore, when users accessed certain Macintosh files, the server crashed. Following this discovery, the server was down for one week for repairs. Students were unable to work on and complete projects for class, faculty had difficulty teaching their classes, and the staff was constrained in their normal day-to-day operations.

Working nearly nonstop for a week, the system administrator performed repairs on the corrupted directories. Assisting him in the work was a contracted consultant from the university's information technology center and consultants from Novell and Arcserv.

The group locked out the server so that no new changes were made to system files.

The system administrator then collaborated with his colleagues to restore data from a three week old backup tape that was uncorrupted and reconcile it with any new files or changes that had been made since the backup. To do this, the group was required to use special tricks and functionalities of the new backup software in a way that wasn't fully intended by the manufacturer. Typically, such tricks aren't recommended for "critical" data.

Following their week of work, the system was fully functional and up-to-date.

Costs and Incident Implications

Our analysis of these events reveals a total quantifiable cost to the university of **$119,300** to **$259,300**. Included in this figure are the workers' costs and new purchases, as well as an estimate of user costs. The wide range of costs in this incident can be attributed to the difficulty in measuring user costs.

Apart from the cost implications, this incident motivated a number of administrative and procedural changes. The school purchased new hardware to run the system. The hope of the system administrator is that some redundancy among machines will prevent further full-system crashes in the future. Each machine will serve different directories, so if a problem occurs in one area, others will be unaffected. The Web page will have its own dedicated server so that if they experience another system failure, people will still be able to access the site.

Although the backup software, ultimately responsible for the crashing system, is considered an "industry best" product, the system administrator now spends a good deal more time evaluating other backup vendors.

Workers' Costs

Three university employees were involved in the incident resolution for 188 hours. Note in Table C-86 that there was no charge for the software consultants; the school was not billed for consulting services. The school paid a contract fee on the university consultant, but because one university entity paid another, it was just an internal transfer of funds. Thus, we only included the university consultant's wage. The staff member included was part of the team configuring software for new machines purchased as a result of the incident.

Table C-86

Workers' Costs					
Title	Hours	Cost/Hr.	Total	-15%	15%
Sysadmin	152	$18.00	$2,736.00	$2,325.60	$3,146.40
Internal Consultant	24	$19.66	$471.92	$401.14	$542.71
Technical Staff	12	$21.30	$255.60	$217.26	$293.94
Subtotal	188		$3,463.52	$2,944.00	$3,983.05
Benefits @28%			$969.79	$824.32	$1,115.25
Subtotal (Salaries + Benefits)			$4,433.31	$3,768.31	$5,098.31
Indirect Costs			$2,305.32	$1,959.52	$2,651.12
Total Labor Costs			**$6,738.63**	**$5,727.84**	**$7,749.43**
Median Cost				**$6,738.64**	**+/-$1010.80**

New Purchases

As a precaution against further crashes, the school purchased three new file servers at a cost of $20,000. The system administrator intimated that, while the new purchases were inevitable, the actual purchases were influenced by the server crash incident. He estimated that the incident was 33% responsible for the decision to purchase new hardware. Therefore, we have included only one-third of the price of the new server purchases in our analysis. The only other purchase associated with the incident was a hard disk, which cost $1,000 (see Table C-87).

Table C-87

New Purchases	
Three new servers	$20,000.00
Percentage attributed to incident	$6,600.00
New hard disk	$1,000.00
Total New Purchases	**$7,600.00**

Users' Costs

The most difficult cost category to measure is users' costs. These costs consist of time lost as a result of the inability to work on projects, classroom material, and so on. A good representation of these costs would include a measure of frustration, aggravation, and stress. To compensate, we have developed a number of reasonable scenarios that provide some sense of what we might find if we possessed all the information we would like to have (see Table C-88). The estimates, while not perfect, are given as a guide for the reader.

All our estimates are based on 275 students, 29 professors, 14 adjunct lecturers, and a staff of 34. Our scenarios assign varying values to the degree of inconvenience the server crash caused each group. To calculate a dollar value, we used the labor market as an allied market for the monetary value of time. Where available, averages on real published salaries were used. Where wage rates were unavailable, we used an average wage rate for a person occupying that position. The final figure we report here is based on an "average user."

Table C-88

User Scenarios			
Student Scenarios	Hours	Value of Time	Subtotal
One	50.00	$12.00	$165,000.00
Two	35.00	$12.00	$115,500.00
Three	20.00	$12.00	$66,000.00
Professor Scenarios			
One	40.00	$44.00	$51,040.00
Two	30.00	$44.00	$38,280.00
Three	20.00	$44.00	$25,520.00
Adjunct Lecturers Scenarios			
One	20.00	$18.00	$6,840.00
Two	15.00	$18.00	$5,130.00
Three	10.00	$18.00	$3,420.00
Staff Scenarios			
One	40.00	$16.00	$21,760.00
Two	30.00	$16.00	$16,320.00
Three	20.00	$16.00	$10,880.00
Subtotal			
Scenario One			$244,640.00
Scenario Two			$175,230.00
Scenario Three			$105,820.00

Total Costs

We estimated total quantifiable costs for the incident by adding the subtotals from the three categories of costs (see Table C-89).

Table C-89

Total Costs				
Workers' Costs			$6,738.64	+/-$1010.80
Users' Costs			$105,000-$245,000	
New Purchases			$7,600.00	
TOTAL COSTS		$119,338.64 - $259,338.64		
Rounded to Nearest $100.00		$119,300.00 - $259,300.00		

Unquantifiable Issues

Of the unquantifiable issues, the blow to the school's reputation is the most problematic. The system administrator reported being besieged by complaints, complaints that injure a school's standing. We know of no way of costing out the effect of diminished prestige, but we are certain that it is damaging. Qualitatively, a diminished reputation may cost a school grant awards, top faculty, and students, as well as years of trying to rebuild its prestige. Fortunately for the school and university alike, the incident did not receive a lot of publicity.

Another issue worth discussing is network reliability. As a result of the incident, students, faculty, and staff began to use their hard drives and zip disks as alternatives to saving files on the network. What worries the system administrator is that a user may have a hard disk crash or zip disk failure and completely lose his or her work. The network servers are backed up many times each day. Even in this incident, no documents were lost forever; they were just suspended for repairs. One can imagine a scenario in which a person could lose more than a week's work and have no backup because he or she didn't trust the system. By the same token, one lightning strike could wipe out much more than a week's work.

GLOSSARY

ABS
Automated Billing System.

ARA
Apple Remote Access, a network protocol that allows dial-in users of Macintosh computers to user AppleTalk over a TCP connection.

bot
Abbreviation for "robot," a program that exists on an IRC channel. A bot can serve either useful purposes, such as administering the channel, or malicious purposes, such as taking over the channel.

CERT
Computer Emergency Response Team, an organization founded in 1988 to work with the Internet community in responding to security incidents.

CF
Cost factor, an element that has been identified as having the potential to increase the cost of an incident.

channel
See "chat room"; see also "IRC."

chat room
The virtual "location" for a group discussion in Internet Relay Chat (IRC) and similar systems. Also known as a "channel." See also "IRC."

CIC
Committee on Institutional Cooperation, a consortium consisting of the member universities of the Big Ten and the University of Chicago.

CIO
Chief Information Officer.

client
A computer system that requests a service of another computer system using a protocol and accepts the other system's responses. See also "protocol" and "'server."

CPU
Central processing unit.

denial of service attack
A type of attack on a computer system that seeks to deny access to the system by legitimate users by, for example, flooding the system with meaningless data.

gateway
An interface between an external source of information and a World Wide Web server.

gopher
A popular distributed document retrieval system.

hacker
A slang term for an individual who tries to gain unauthorized access to a computer system. Computer enthusiasts use the term to apply to all persons who enjoy programming and exploring how to expand their programming skills. Those who use the broader definition of "hacker" call those who engage in unauthorized activities "crackers.'"

http
Hypertext transport protocol, a protocol used for moving data on the World Wide Web. See also "protocol."

ICAMP
Incident Cost Analysis and Modeling Project.

ICR
Indirect cost rates.

ID
A unique identifier, usually a name or number.

IFS
Institutional File System.

IMAP
Internet Message Access Protocol, a protocol that allows a client to access and manipulate electronic mail messages on a server.

incident
For the purposes of this study, any event that takes place through, on, or constituting information technology resources that requires a staff member or administrator to investigate and/or take action to reestablish, maintain, or protect the resources, services, or data of the community or individual members of the community. See also "information technology resources."

information technology resources
Those resources, both tangible and intangible, that are related to computer systems and networks, including computer hardware and software, peripherals, and the institutions (administration and employees) that are established to operate the systems.

Internet
The worldwide collection of networks using the TCP/IP suite of protocols.

intranet
A network that provides services within an organization that are similar to those services available on the Internet. An intranet is usually not connected to the Internet and is usually accessible only by those within the organization.

IP
Internet Protocol, the network layer for the TCP/IP protocol suite. See also ."protocol" and "TCP/IP.'"

IP address
The numerical address of a host computer on the Internet. See also "Internet" and "IP."

IRC
Internet Relay Chat, a system of large networks that allow multiple users to have typed, real-time, online conversations.

ISDN
Integrated Services Digital Network, a set of standards for a high-speed data connection that can carry voice, digital, and video signals across a single wire or optic fiber.

ISP
Internet Service Provider, an organization that provides access to the Internet.

IT
Information technology.

ITO
Information technology ombudsman.

LAN
Local area network, a data communications network that is limited to a small area.

login machines
Computers which enable users to gain initial access to a computer network.

mail bomb
An immense amount of electronic mail sent to a single computer system or person with the intent of disabling the recipient's computer.

NLM
Network Loadable Module.

OF
Occurrence factor, an element identified as having the potential to increase frequency of occurrence of incidents.

PC
Personal computer.

PPP
Point-to-point protocol, an Internet standard for using TCP/IP over point-to-point connections. See also "protocol."

protocol
A set of formal rules for transmitting data, especially across a network.

server

A computer system that provides a service to other computer systems connected to it over a network. See also "client."

sniffer
A network monitoring program that captures and decodes data packets.

TCP
Transmission Control Protocol, a network, protocol governing sequenced data. See also "'protocol."

TCP/IP
Transmission Control Protocol /Internet Protocol, a suite of protocols developed originally by the Advanced Research Projects Agency and used on the Internet. These protocols include File Transfer Protocol and telnet. See also "protocol."

Trojan Horse
A malicious program that is disguised as something harmless.

UPS
Uninterruptible power supply.

URL
Uniform Resource Locator, a means for specifying the location of an object on the Internet.

WAREZ site
A (usually) compromised computer account that software pirates use to distribute copyrighted software illegally.

World Wide Web
An information retrieval system on the Internet. Also referred to as “WWW” or “the Web.”