



Computer Security Case Doctors Hospital: The Information System

prepared for

Detmar Straub, Ph.D.
CIS 869

by

Leigh Cameron
Mark Carter
Jamie Kohm

February 29, 1996

NOTE: This case was prepared for the purpose of class discussion rather than to illustrate the effective or ineffective handling of an administrative situation.

CONTENTS

DOCTORS HOSPITAL: THE INFORMATION SYSTEM	1
BACKGROUND.....	1
REQUIREMENTS FOR THE NEW INFORMATION SYSTEM	4
RECOMMENDATIONS	8
DISCUSSION QUESTIONS	9
EXHIBITS.....	10
COMPUTER SECURITY POLICIES	20

Doctors Hospital: The Information System

“If we are to compete in the 1990’s and beyond, we must look to information technology as an enabler of our business strategy. We have been in the dark ages of technology for too long. I only hope it is not too late for us to catch up. We have the best medical equipment, why not the best computer equipment? Something has to be done, and we must move quickly.”

- Edward E. Lynch, Chairman of the Board, Doctors Hospital

In July 1995, Paul Davis, Vice President, Information Systems, reflected on the enormous project facing his systems group. The Board of Trustees had voted to pursue updating the hospital’s information system in the recent quarterly meeting. This action was championed by Chairman Ed Lynch who had just returned from visiting St. Elizabeth’s hospital in Chicago. Lynch was a wealthy and influential trustee who held a tight reign over the Board. Lynch did not like being second best and what he saw at St. Elizabeth’s convinced him that Doctors Hospital was not up to par when it came to information systems.

Paul rubbed his temples in contemplation. He and his systems group were in the spotlight. With Ed Lynch leading the parade, Paul was under intense pressure to develop a system that would meet the Board’s expectations. The hospital’s President, Allen Weis, had given Paul three months to develop requirements for the new information system. Specifications were to be presented to several vendors for bids no later than October 31st.

Paul was not optimistic that specifications could be developed in three months. The information systems department was both understaffed and underfunded. Paul had replaced the previous V.P. of Information Systems, Walter “Wally” Belzer, just three months earlier. From April to July, Paul had accomplished little. There was little documentation on the existing system and what did exist was unintelligible. Wally had left Paul a mess.

Background

Wally had been with Doctors Hospital for fourteen years. He joined the hospital in 1981 as a contract programmer when the first computers were introduced to the hospital. He designed most of the hospital’s system applications for the IBM System 370 mainframe. As it became apparent that Wally was critical to the operation of the information system, he was hired as a permanent employee. He eventually became

V.P. of Information Systems in the mid-eighties since he was the only one who understood how the system worked. In early 1995, Wally resigned in order to pursue his life-long dream to back-pack through Europe.

Wally's resignation was quite a shock to the hospital's President, Alan Weis. Weis depended on Wally and was unprepared to recruit a replacement. Weis was not computer savvy, nor did he feel a pressing need to become so. That's what he had an information systems department for. Weis reflected:

"It was sheer luck that I found Paul! Paul was a local boy that went away to college some years ago. He and his wife had just moved back to town to be closer to Paul's aging folks. He's a young guy, maybe 30 years old. He had done something in computers back in Atlanta, so I grabbed him! We don't find too many computer types in Beaver Creek . . . it's more of a blue collar town."

Paul was flattered by the job offer, Vice President of Information Systems sounded pretty impressive to the former computer systems consultant. He accepted without hesitation. There weren't a lot of opportunities for information systems professionals in Beaver Creek. He had assumed he would have to make the hour and a half commute to Springfield to find a suitable position. The job at Doctors Hospital would enable him to spend more time with his family.

It had taken Paul three months just to get his small office organized and develop some grasp of the information flows in the current system. He began to regret that he ever accepted the position at Doctors Hospital. Everything was a mess. Wally's system made no sense to Paul. On July 15th, he began charting the information flows of the current system. "If I write everything down, maybe it will start to make sense," Paul thought to himself.

It soon became clear that something was unusual about Wally's legacy system. As Paul was balancing the data flows in the patient accounting system, he became increasingly frustrated that his accounts were out of balance by small dollar amounts. Too small to worry about on individual patient accounts, but Paul was concerned that the sum of these discrepancies would represent a tremendous amount of money.

Upon further investigation, Paul discovered an "automatic" small balance write-off account. There was a small program imbedded in the system that would target random patient accounts when payments were applied. The payment amount would be entered by the data-entry clerk at the full amount; however, when the payment was posted a small percentage of the account would be "shaved" off and applied to a hidden account. A corresponding amount would be written off to the small balance account. These small balance write-offs were not suspicious because it was hospital policy to write off any patient balance under two dollars to save the administrative costs of processing the statements.¹

¹ This is an actual policy at a hospital in metro Atlanta (name withheld as requested by the source).

Paul was virtually certain that Wally had used the computer system to embezzle money from the hospital.² According to Paul's calculations, the hospital may have lost in excess of two million dollars in the fourteen years Wally had been working there (See Exhibit 3). Paul was hesitant to go to President Weis with this information because he couldn't absolutely prove that Wally was the culprit. Paul couldn't quite figure out how this hidden account worked and where the money was diverted to.

The stress was getting to Paul, he was working fourteen hour days and barely sleeping. He only had two and a half more months to get the specs ready for the new system and he was spending all of his time playing detective on the old system! One night, Paul bolted upright in bed. The payroll system! It had come to him in a dream - maybe Wally had corrupted more than just the patient accounting system?

Two days later, Paul found what he was looking for. Wally had directed the funds from the patient accounting system to a dummy account in the payroll system. Because the hospital had a direct deposit arrangement with the local bank, diverted funds were automatically deposited to a local account. Each pay period, Wally transferred the balance of this account to a numbered account in Switzerland. When he had fully uncovered the scheme, Paul exclaimed, "That little weasel didn't dream of back-packing through Europe, he wanted to go first class!"

Now that he had all of the facts, Paul was ready to go to President Weis with the information. The encounter was not what Paul expected. Weis was outraged:

"We've got to put the lid on this. I can't believe I was duped! This conversation doesn't go out of this room. Do you understand what this would do to the hospital's reputation? Don't breath a word, do you hear me? Just do your job. I don't remember 'detective' anywhere in your job description! You've wasted valuable time you should have been spending on those new system specs Lynch wants."

Paul was dumbfounded. He didn't know what to do. He thought he would be a hero. Hadn't he just uncovered a two million dollar theft? Should he go over Weis' head to the Board? Paul left the hospital that afternoon demoralized. He sort of understood Weis' position, but it still made him feel uneasy. Paul knew that often computer crimes were not reported to the authorities because of the company's fear of appearing incompetent.³ He also knew how important it was for patients to have trust in and feel safe at their local hospital. Publicity surrounding Wally's crime could be devastating. Besides, Paul rationalized, Wally wasn't even in the country any more. Thankfully, it was Friday and he didn't have to face Weis again for a few days.

² This is referred to as a "salami attack." See: Forcht, Karen A. Computer Security Management. Danvers, Massachusetts: boyd & fraser publishing company, 1994, p. 16.

³ Forcht, p. 11.

Requirements for the New Information System

On Monday, Paul was determined to channel all of his energy into developing the specifications for the new system. His wife had encouraged him not to 'rock the boat' and just try to do the job he was hired to do.

Paul began by interviewing the functional department heads to try to understand what their information requirements were, what needs were currently met by the old system, and what enhancements they might want in the new system. Paul spent a full day with each of the other eight functional Vice Presidents documenting their needs. Paul spent several more days just watching the information flows among the departmental users. With less than two months until his deadline, Paul had merely begun to draft his list of information requirements.

Vice President Finance

Paul's first meeting was with Sam Lee. Sam had been with the hospital for only two years and was frustrated by the poor audit trails. When Paul approached him about his department's information needs, Sam was elated.

"I can't believe we're really getting a new system! The audit controls in this one are terrible. There is no separation of duties and the data available from our system is worthless. I wake up every morning wondering if this will be the day the sky will fall down! We're on thin ice with this system. Numbers don't balance and I'm constantly making adjustments that just don't seem quite right. I can't get any support from Weis either. 'Just balance the books,' he says, as if I were just a junior accountant! Sometimes I wonder what the man is thinking."

Paul developed an immediate rapport with Sam. Sam understood both the problems and the urgency for changing the ways things were currently done. Sam wanted the financial applications housed on a separate server with tight access controls. Sam was also concerned about risk assessment.

"People around here don't recognize the potential threats to the system. Back-ups aren't done as often as they should be. Even if the tapes were current, they are stored right here in the hospital. What if there were a fire? You have to think about these things if you are going to protect your information assets."

Paul suggested to Sam that they should get a group together to develop a contingency plan for disaster recovery. They considered using the threat scenarios methodology to stimulate thinking about potential dangers. We need to ask two questions, Sam said:

*“What is the worst thing you can imagine happening?” and
“What is the most likely thing to happen?”⁴*

Vice President Planning and Marketing

Paul's next meeting was with Phil Roberts. Phil was also new to Doctors Hospital, having just joined the staff in June, 1995. He was recruited by Ed Lynch to help update the hospital's image. Competition from hospitals in neighboring communities was a growing concern. Beaver Creek residents would often drive in excess of thirty miles to seek care at what they perceived were 'newer and better' hospitals.

Phil was a highly motivated individual who was eager to assist Paul in developing requirements for the new information system. Phil had a lot of ideas.

“I want to get closer to my customers, the patients and the doctors. I want a database where I can capture demographics and preferences. I want to be able to run reports to show where my patients are coming from, what they do for a living, and what their responses were to the patient satisfaction questionnaire. This will show me what market segments are under-served by the hospital, and where to target our marketing campaigns and direct mailings. I want a dynamic interface with this information.”

“I also want applications on my desk-top so I can develop presentations and in-house marketing materials. Our department can be more responsive to the hospital's needs with these capabilities at our fingertips.”

Vice President Public Affairs & Development

Lisa Franklin had been with Doctors Hospital since 1987. Lisa served as a liaison between the hospital and local community. She was concerned with projecting a positive image of the hospital and in developing new programs to meet the needs of Beaver Creek residents.

Lisa wasn't extremely interested in meeting with Paul. She thought the current system was just fine, but she conceded that she would like a better word processing application.

⁴ Straub, Detmar. CIS 869 Course Notes, January 16, 1996.

Vice President Medical Services

Paul was somewhat let-down after his meeting with Lisa and was not looking forward to his next appointment was with the venerable Dr. Jim Payne. Dr. Payne was appointed Vice President of Medical Services in 1978 and was well-respected both in the hospital and in the community.

Dr. Payne wanted improved information services for the medical staff. He wanted to see the hospital move from a paper to an electronic medical record. Dr. Payne also wanted a voice transcription application called VoiceEM. Ed Lynch had seen this technology in action at St. Elizabeth's hospital and had described to Dr. Payne what it could do:

"This thing is great. VoiceEM provides the physician with a menu of common medical complaints, you select the appropriate situation and then the system prompts you with questions. You respond right into a microphone . . . this thing has a built in medical vocabulary of 1,000 words and can be trained to recognize each doctor's voice. In less than one minute, a signature ready report appears on the screen which you can edit from the keyboard.⁵ This would sure make dictating operative reports easier and faster."

Vice President Patient Services

Hannah Harris had a nursing background and had recently finished her MBA at Indiana University. Hannah was a vibrant and proactive individual who put the needs of patients above all else.

Hannah was anxious to provide on-line services in patient hospital rooms. She wanted patients and/or patient families to be able to get information on their condition, send e-mail to their physician, and pull up a schedule of when their next medication, nursing check, or physician visit was scheduled for. She believed that this type of system would eliminate some of the anxiety patients and family members feel in the hospital because they spend so much time waiting.

Vice President Facility Development

William Scott was not excited about the prospects of installing a lot of new hardware in the hospital. He had been with the hospital for twenty years and remembered the difficulties the hospital had experienced with the installation of the first computers in 1981.

⁵ Alter, Steven. Information Systems: A Management Perspective. Reading, Massachusetts: Addison-Wesley Publishing Company, 1992, p.199.

He told Paul during their interview that he did not understand the need to put a computer in virtually every room in the hospital. This would mean space planning, re-wiring, and enhanced physical security controls. Paul soon discovered that William Scott wasn't enthusiastic about projects which affected 'his' facilities unless those projects were Scott's own idea.

Vice President Human Resources

Sandra Brown had come up through the ranks to become Vice President of Human Resources in 1990. Sandra was a self-starter who began her career with the hospital in 1979 as a patient registration clerk while she was attending community college in the evenings.

Like the Information Systems department, Human Resources was badly understaffed. The department consisted of Sandra and two administrative assistants. Sandra's group was responsible for all of the pre-screening of prospective employees, administering of employee benefits, and entering/updating employee payroll information. In addition, they had recently been giving the responsibility of developing counseling programs for hospital employees.

When Paul approached Sandra about her department's information needs, she laughed. Sandra vividly illustrated the information flow in her department:

"Our business is information. We are swamped with papers and files in this tiny office! Payroll is automated, but errors are frequent and we spend a lot of time making corrections and getting manual payroll checks generated. All of the employee benefits information is administered manually. There is just too much paper. We spend half of our time looking for things. You may have to look in three different files to get the information on one employee. Payroll files, benefits files, and personnel files are all separate. I certainly don't have time to develop employee counseling programs!"

Paul thought that a transactional processing system for the payroll accounting and an imaging system for employee records, combined with access tools which would create dynamic links between the two systems, might just be the answer to Sandra's problems.

Vice President Nursing

Paul's last interview was with Patricia Clark. Patricia had been a surgical nurse for fifteen years prior to her appointment as Vice President of Nursing in 1981. Patricia shared Dr. Payne's enthusiasm for an electronic medical record. She also wanted an improved patient registration and tracking system. Patricia also had some ideas about

combining an inventory management application with a physician preference card system to improve ordering and reduce errors in pulling supplies for surgery.

Recommendations

It seemed to Paul that a distributed computing environment was what was needed at Doctors Hospital. A client/server architecture would be a dramatic change from the current mainframe platform. Dumb terminals would be replaced with networked microcomputers and users would have the power to do more of their own processing and ad hoc reporting. Paul believed that the hospital should purchase off-the-shelf applications/code and integrate with the legacy system where possible. The new system was going to be both expensive and time-consuming to implement.

Paul presented his requirements for the new system to Allen Weis and the Board on October 29th, just two days before his deadline. The Board members were thrilled by the new capabilities, but not the estimated cost. Requests for purchase were submitted to three vendors. Bids were to be submitted to the hospital by November 30th. Paul projected that the implementation of the new system would occur in four phases over a two year period.

Paul was concerned that the Board did not understand the security issues that would be created by the new system. There was currently no computer security function within the Information Systems department and Paul worried that funds would not be made available for him to hire a much needed Computer Security Administrator. Paul reflected on his confrontation with Allen Weis:

“Weis said that ‘detective work’ was not part of my job, but it is. Computer security is everyone’s job. People have become more comfortable using computers, but don’t seem to understand how important it is to protect their information resources. There are so many threats out there and Wally Belzer is just one example. The biggest threats to computer security are caused by losses due to human errors, accidents, and omissions.⁶ Not only must we build in audit controls and variance checking into our new system, but we must also train our users and create a heightened awareness of the vulnerabilities we face.”

Paul expressed these concerns to Bill Johnson, Executive Vice President and Chief Operating Officer. Bill suggested they form a team made up of members from each functional area to start developing policies for computer security. Bill believed that they should start conducting user awareness training regarding computer security as soon as possible.

⁶ Forcht, p. 66.

Paul was relieved. Finally, someone was on his side. He began to look forward to the conversion to the new system even though it would mean he would continue putting in long hours at the office. At least he would believe in what he was doing. As for Wally, he got away with his elaborate scam, but Paul was determined not to let it happen again.

Discussion Questions

1. If you were Paul, would you have gone over Allen Weis' head to the Board with your accusations against Wally?
2. Do you think that the hospital should implement a computer security department? And if so, who should this department report to?
3. What type of physical security measures would you implement in a hospital with such an open environment?

Exhibits

1. Organizational Chart - Doctors Hospital
2. Organizational Chart - Information Systems Department
3. Estimated Loss from Wally's Computer Theft
4. Computer System Configuration
5. Computer Threats Diagram
6. Computer Crime
7. Industry Penetration of Contingency Plans
8. Hospital Brochure
9. Postcard from Wally

Exhibit 1.

Organizational Chart
Doctors Hospital
June 30, 1995

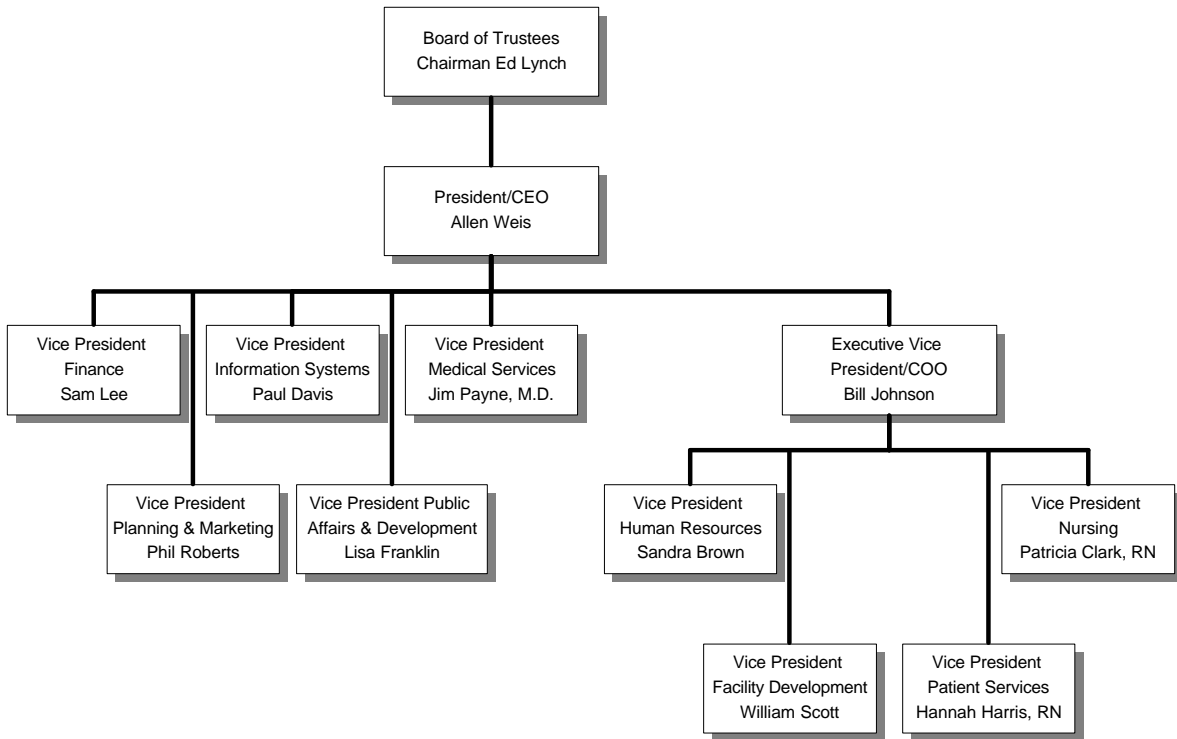


Exhibit 2.

Organizational Chart
Information Systems Department
June 30, 1995

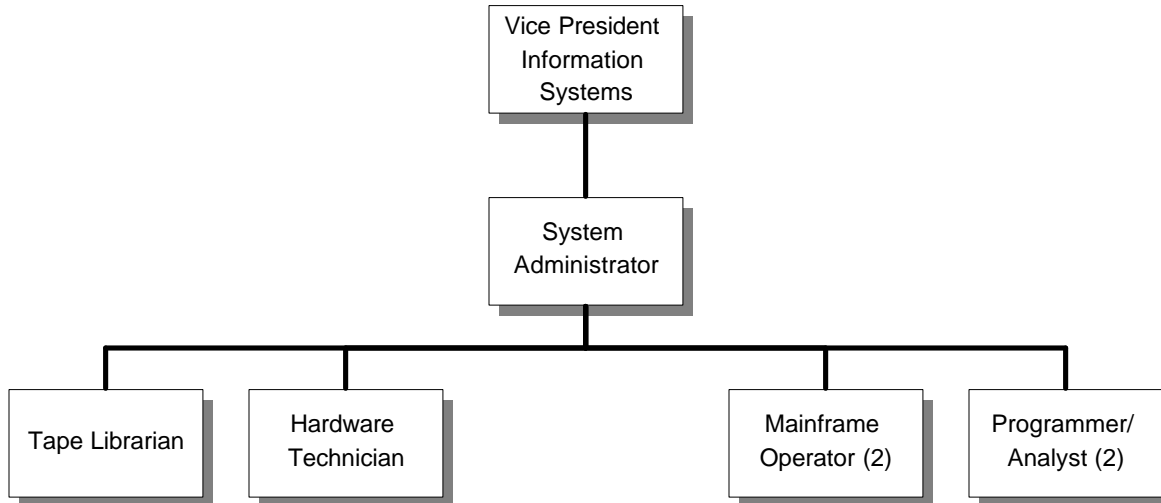


Exhibit 3.

**Estimated Computer Abuse Losses to Embezzlement
by Wally over 14 years of employment**

Estimated Customer Write Offs (for time period prior to bank records)		
Write Offs of Small Balances (under \$2):		
Write Off Amounts	2,145.00	
Number of Weeks	<u>52</u>	
Total Yearly Loss	111,540.00	
Number of Years	<u>7</u>	
Total Estimated Loss		780,780.00
Bank Records		
Actual Funds Transferred Through Account within last seven years:		<u>1246821.29</u>
Total Estimated Losses to Computer Embezzlement		\$ 2,027,601.29

Exhibit 4.

**Doctors Hospital
Computer System Configuration
June 30, 1995**

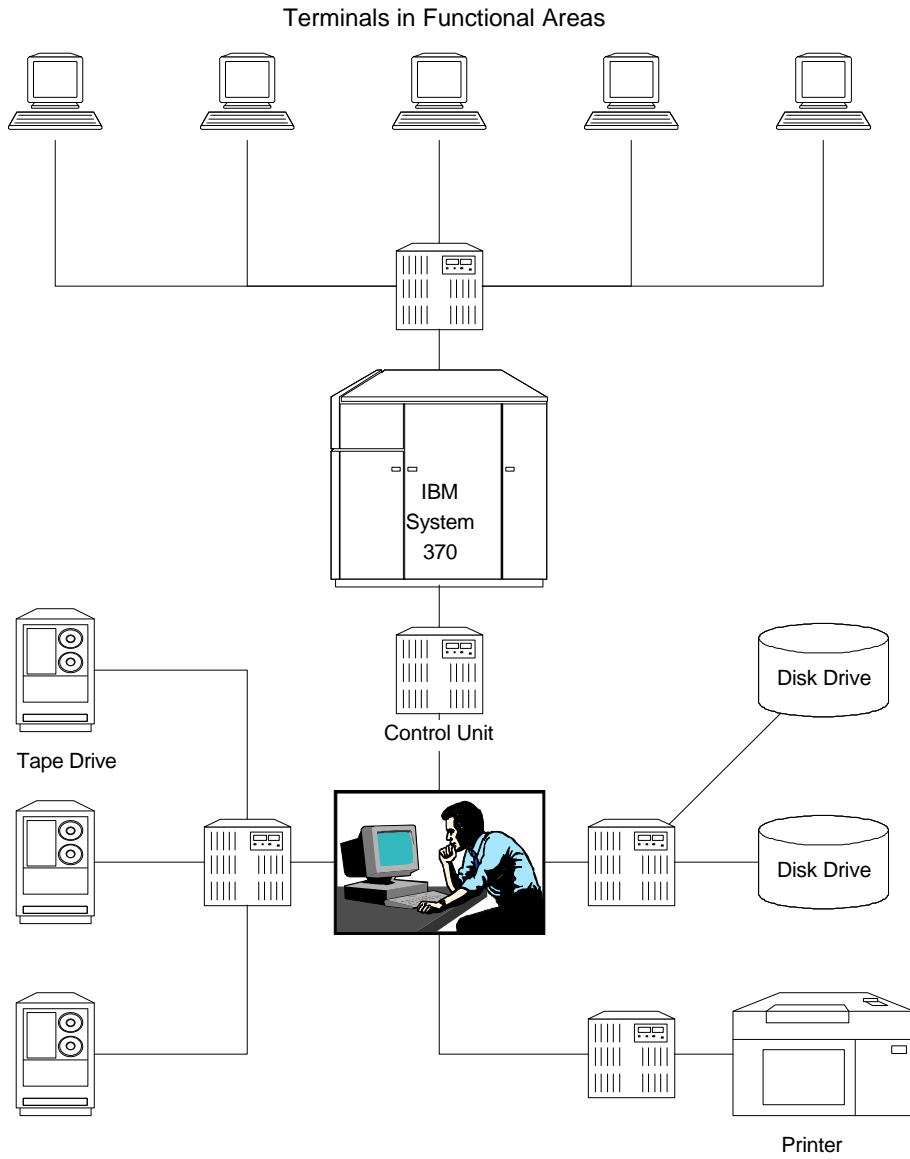
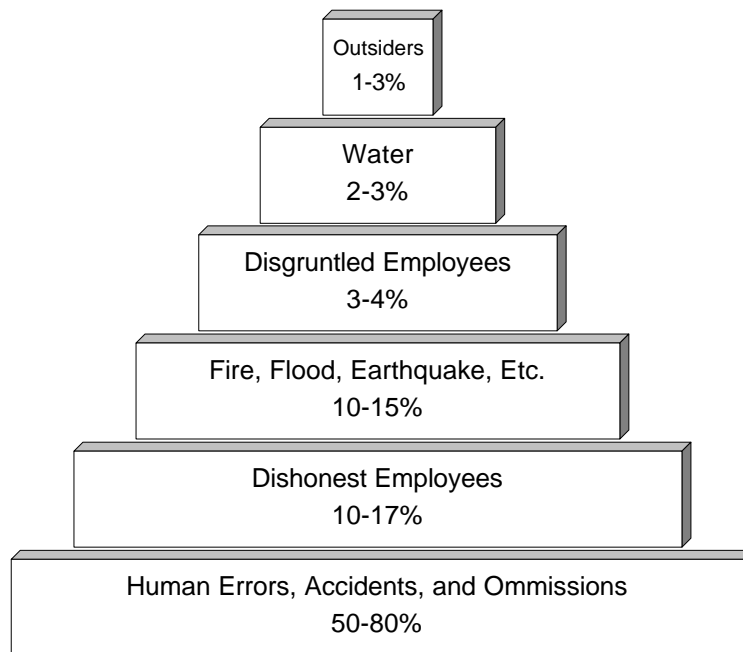


Exhibit 5. Computer Threats

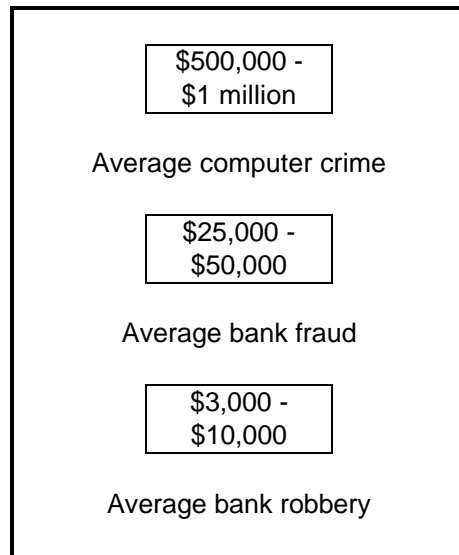
Where Do The Computer Losses Really Occur?



Source: Forcht, Karen A. Computer Security Management. Danvers, Massachusetts: boyd & fraser publishing company, 1994, p. 66.

Exhibit 6.

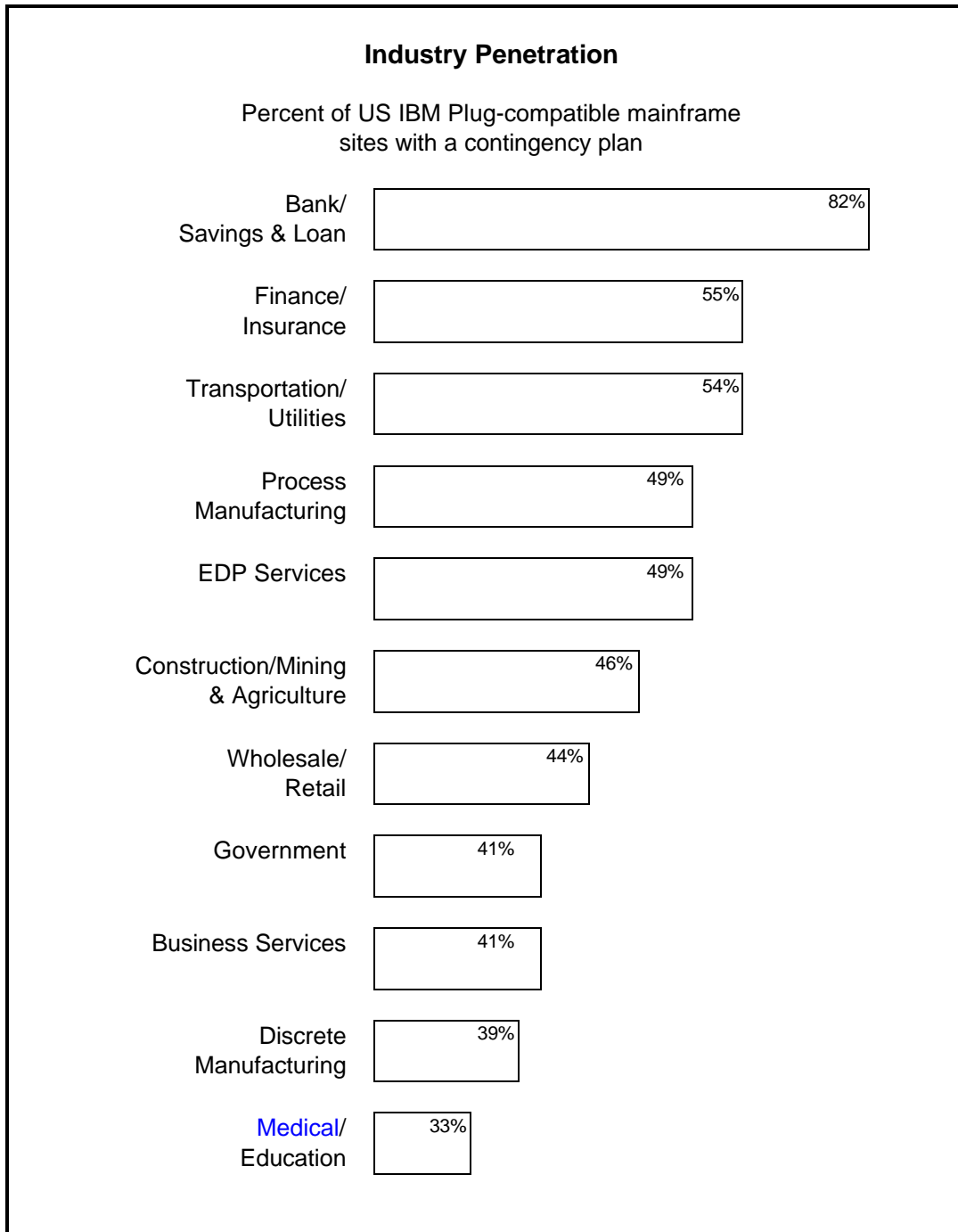
Comparing Computer Crime to Other Major Crimes



Source: Forcht, Karen A. Computer Security Management. Danvers, Massachusetts: boyd & fraser publishing company, 1994, p. 297.

Exhibit 7.

Industry Penetration of Contingency Plans



Source: Peter D. Anderson, "Disaster Planning . . . The Need for an Integrated Approach," *Computer Control Quarterly*, Vol. 9, No. 3, 1991, p. 37.

Exhibit 8.

**Hospital Brochure
June 30, 1995**

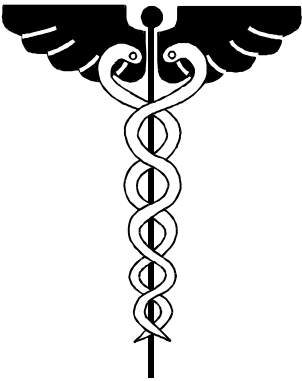

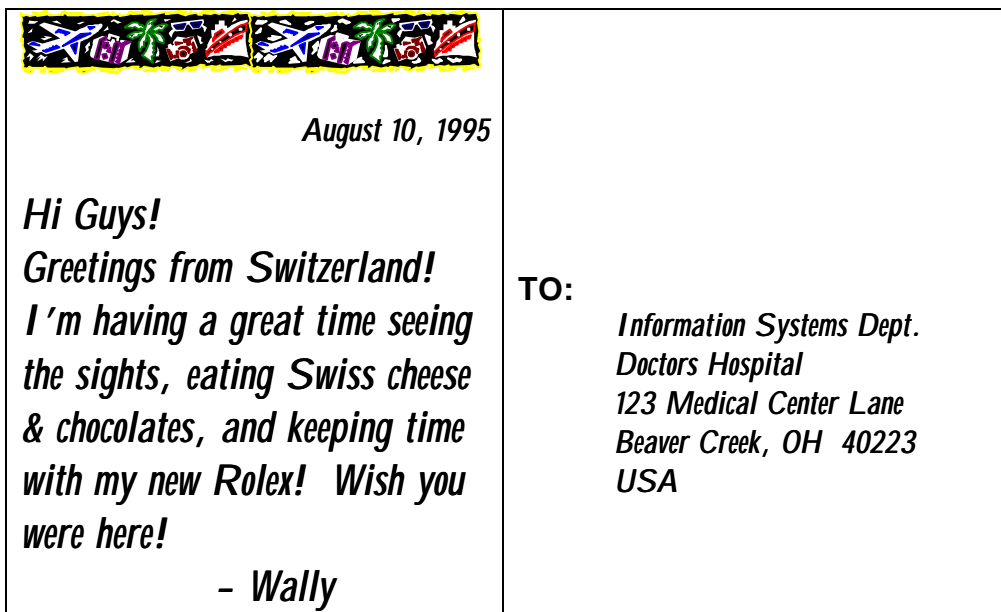
<p>Doctors Hospital 123 Medical Center Lane Beaver Creek, Ohio 40223</p>  <p><i>“Our mission is your good health”</i> - Edward E. Lynch Chairman, Board of Trustees</p>	<p>At Doctors Hospital, we believe in providing the highest quality care to our patients. As a patient, you are the most important person in this hospital.</p> <p>We believe that your good health is our primary concern!</p> <p>This is demonstrated in our commitment to a highly trained and caring medical staff. In addition, we are committed to maintaining a nurse-to-patient ration of one to ten to ensure that our patients get the personal attention they deserve.</p> <p>At Doctors Hospital, we are committed to the Beaver Creek community as well as our patients.</p>	<p>We have been Beaver Creek’s primary hospital for nearly five decades and are proud of our accomplishments in the community. From sponsoring blood drives and food banks for the poor, to assisting local companies in developing employee wellness programs, Doctors Hospital has invested in your well-being.</p> <p>We want to be your choice for hospital care. At Doctors Hospital, we care about our patients and it shows!</p> 	<p>“I am committed to making Doctors Hospital the facility of choice for Beaver Creek residents, and that means making the patient our first priority.” - Allen Weis, President</p> <p>We have the facilities and staff to support many surgical specialties, including:</p> <ul style="list-style-type: none">- General Surgery- Obstetrics & Gynecology- Ear, Nose & Throat- Orthopedic Surgery- Gastroenterology- Urology <p>We also have excellent emergency care facilities.</p> <p>For additional information or for a physician referral, please call our patient services department at:</p> <p>(215) 228-8687</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Exhibit 9.

Postcard from Wally



Computer Security Policies

Note: The following sample security policies have been developed to protect Doctors Hospital by serving as a deterrent to computer abuse. After reviewing these sample policies and rationale, the reader should be able to develop several additional computer security policies for Doctors Hospital which address areas of vulnerability presented in the case.

I. User IDs and Password Controls

I.1. User IDs and password access controls.

Policy Statement:

All computer systems and sensitive applications must utilize user ID and password tables. In addition, all applications developed in-house must utilize a shared user ID and password table. Applications purchased off-the-shelf should be interfaced with the shared user ID and password table if possible.

Sanctions:

None

Rationale:

User IDs provide a way to control access to applications and data by requiring each user to log into an application upon startup. This will prevent unauthorized use of hospital applications and data. This policy will also prevent unauthorized users from intentionally or unintentionally corrupting data. In addition, it will allow access log files to be created and user ID stamps to be applied to transactions.

I.2. User passwords must be changed every thirty days and they cannot be repeated.

Policy Statement:

All users will be required to change their user passwords at least every 30 days. User passwords will be recorded in an encrypted history file by user ID. Users will not be permitted to reuse previous passwords.

Sanctions:

Denied Access.

Rationale:

In order to eliminate some of the unauthorized access by users who obtain passwords illegitimately, each user will be required to change their password regularly. Users will be instructed not to share their passwords with other users or write them down and leave them lying around. This policy will provide a preventive measure against unauthorized access to hospital computer systems.

I.3. Password Format

Policy Statement:

All user passwords must be at least five characters in length and must include at least one numeric character and one alpha character.

Sanctions:

Passwords which do not conform to this policy will not be accepted and the user will be denied access.

Rationale:

In order to make it harder for a password to be guessed or hacked, the password length will be at least five characters. This will increase the number of attempts needed to determine a password. By using alphanumeric characters the character set is increased to 36 characters, thus increasing the number of possible combinations. Alphanumeric characters will also decrease the possibility of successfully exhausting the dictionary in an attempt to determine a password.

II. Configuration Management

II.1. Configuration management will be used to track both current and future systems.

Policy Statement:

A configuration management database will be used to track the current state and future changes to the following areas:

- Hardware
- Software
- Firmware
- Design and user documentation
- Software tests

Any changes made to one of these areas must be accounted for in the database.

Sanctions:

Failure to comply with this policy will result in a written reprimand which will be added to the employee's permanent record and reflected in the employee's annual performance review.

Rationale:

Configuration management will help eliminate some of the unintentional threats to hospital system assets. These threats include inadvertently deleting program versions, using a prior release of a program and corrupting data, restoring a workstation configuration after a power loss, etc. Configuration management will also help guard against malicious intrusions such as a program be replaced with another version containing a virus or bug, intentional deletion of programs, and in determining components that may have been stolen, etc. A configuration management database could also help the hospital recover after a disaster. The configuration management system may also be interfaced to an inventory/asset tracking system to eliminate duplicate entry and databases.

III. Audit Logs

III.1. Application audit logs

Policy Statement:

All financial applications must generate an audit log that will contain specifics about any transactions processed including, but not limited to, user ID and date/time stamps.

Sanctions:

None

Rationale:

Audit logs will help in resolving problems with a system by providing a synopsis of what transactions were processed. These logs will be useful when trying to determine misuse of the system, including incorrect access levels, fraudulent transactions, user access time, etc.

IV. Information Systems Purchasing

IV.1. Software Purchasing

Policy Statement:

The purchase of all software must be approved in writing by the Information Systems department.

Sanctions:

Installation of any unauthorized software applications on hospital computers shall be grounds for a minimum of a written warning which will become a permanent part of the employee's personnel record. In addition, any such software will be removed from hospital computers upon discovery.

Rationale:

Software is purchased only with the written approval of the Information Systems department to ensure that the application ordered is both necessary and compatible with the hospital's operating system. This policy also protects against potential viruses resulting from an employee installing an infected program on a hospital computer.

IV.2. Off-the-Shelf Applications

Policy Statement:

Applications must only be developed in-house when there are no viable off-the-shelf alternatives available.

Sanctions:

None.

Rationale:

The use of off-the-shelf applications reduces both internal development and maintenance costs. Commercially available software has been thoroughly tested, is widely compatible, and is generally supported by the vendor. This policy also protects the hospital in the case where an in-house programmer leaves the company, taking with him/her the knowledge of how to run and/or maintain the software. Purchasing off-the-shelf applications also limits the risk of in-house developers inserting a trap-door in the software that may be used to exploit the system.

V. Organizational Policies

V.1. Computer Security User Training

Policy Statement:

All employees are required to attend computer user awareness training. This training is to be provided to each employee upon orientation and thereafter on a semi-annual basis. Training will be conducted by the Information Systems Department.

Sanctions:

All employees are required to attend the training sessions. If an employee misses a session, a verbal reprimand from the employee's supervisor is required. If an employee misses two sessions, a written reprimand is required which will become a permanent part of the employee's personnel record. Persistent resistance to computer security training may be grounds for termination.

Rationale:

User awareness training is necessary to advise employees of the need for computer security within the hospital. The training is intended to be both an educational preventive to computer misuse and a deterrence to intentional computer abuse. Computer security awareness training informs users of the threats to the hospital's computer assets and information. Such training also places the burden of computer security on all employees, not just those in the information systems department.