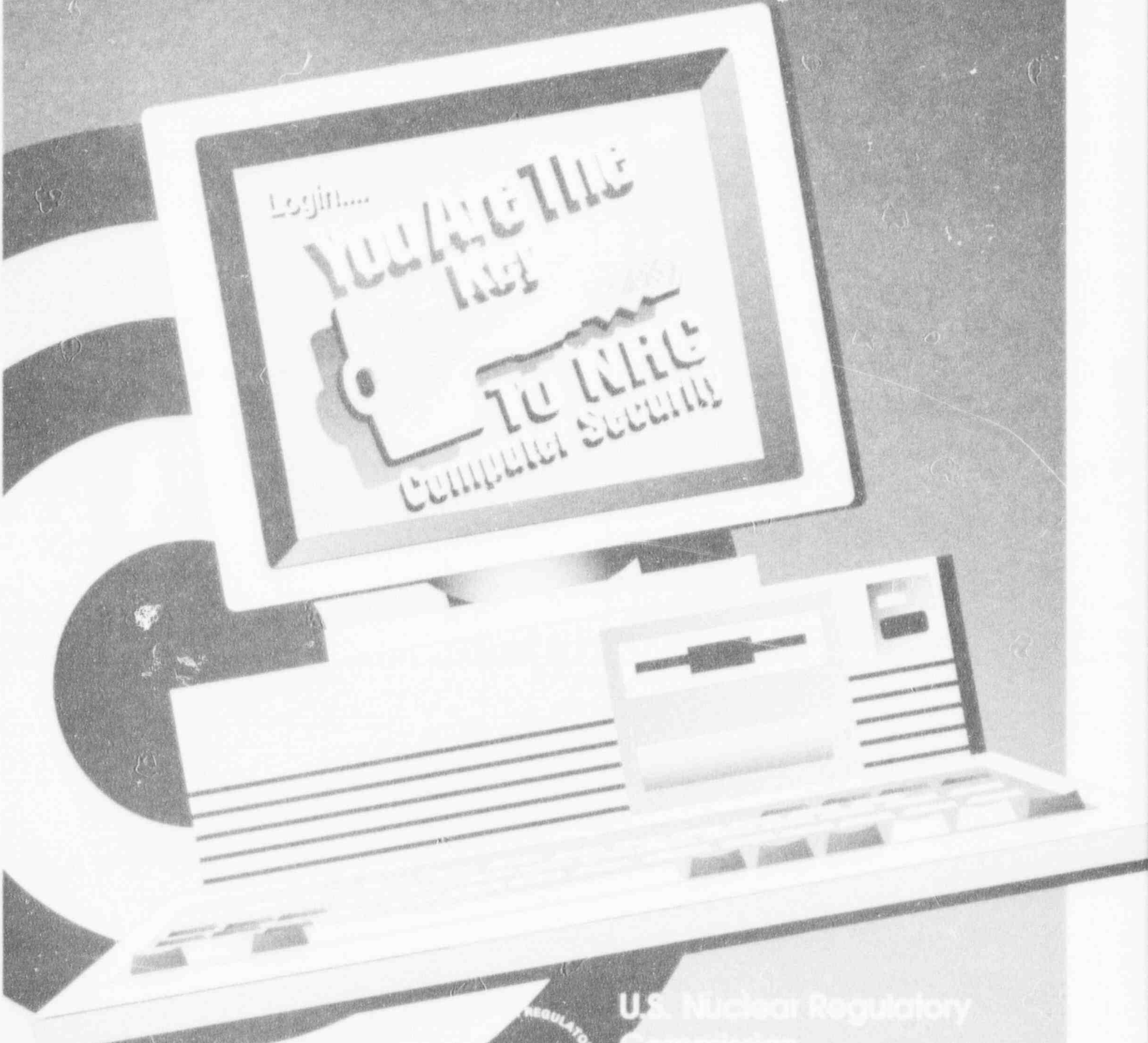
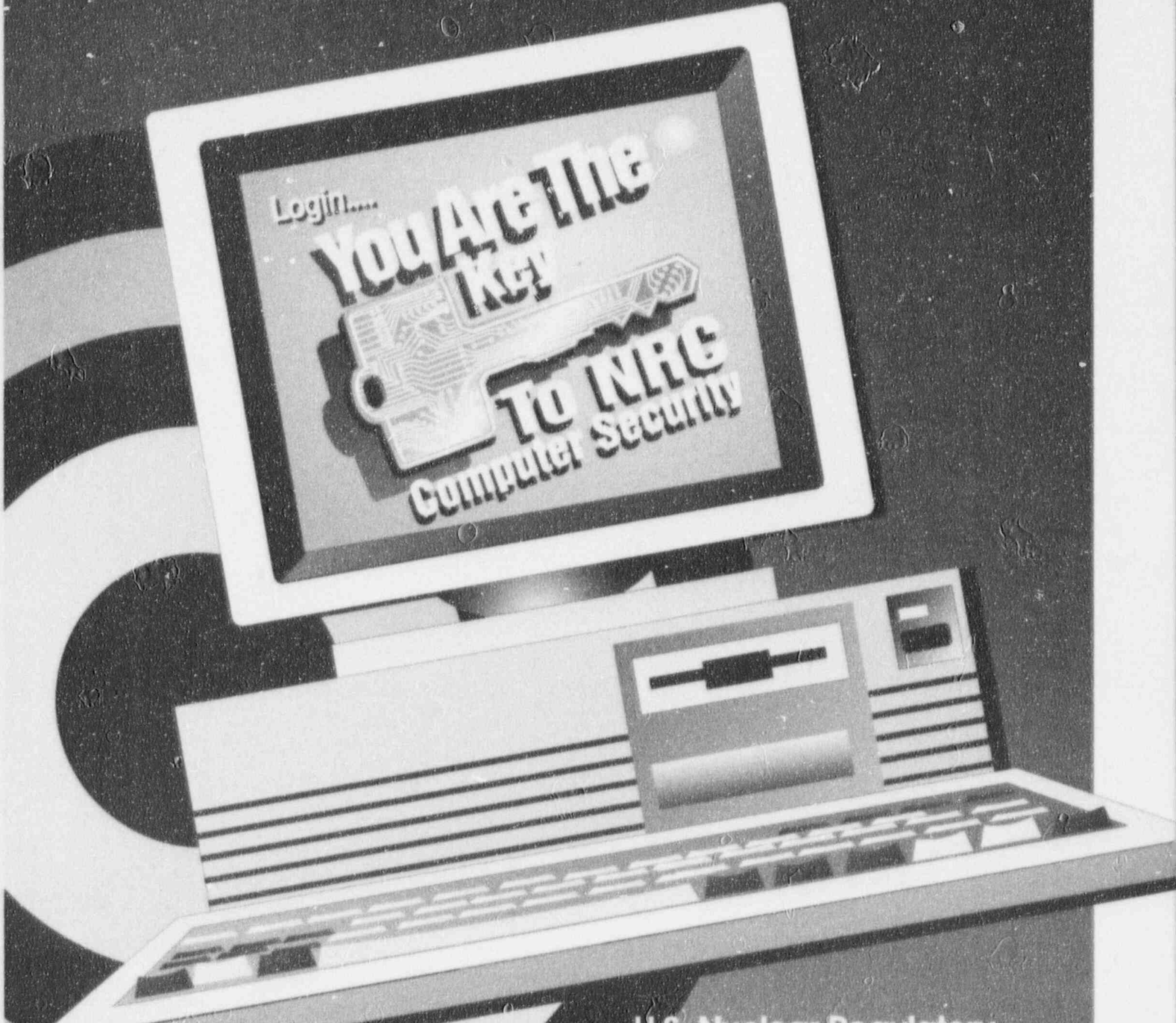
Controlling Computer Threats



U.S. Nuclear Regulatory Commission
Office of Information Resources Management

IF02 0/1

Controlling Computer Threats



U.S. Nuclear Regulatory Commission

Office of Information Resources Management

CONTROLLING COMPUTER THREATS

THREAT AWARENESS

U.S. Nuclear Regulatory Commission

Introduction

This document presents U.S. Nuclear Regulatory Commission (NRC) employees with scenarios of various threats to the local area network (LAN) and microcomputer workstations. Risk assessments and other NRC activities have yielded information on possible environmental threats and system vulnerabilities. The resulting threat scenarios contained in this booklet represent basic threats that could happen at NRC if proper policies and procedures are not followed, or if proper controls are not used correctly.

A threat can be any person, object, or event that could cause damage to a system. Threats can be malicious, such as the intentional modification of sensitive information, or can be accidental, such as an error in a calculation or the accidental deletion of a file. Threats can also be acts of nature, such as flood, wind, or lightning.

One of the overriding vulnerabilities in any system is the lack of user awareness regarding the types and consequences of threats. Although users may understand the need for maintaining confidentiality and integrity of information, they may not be familiar enough with the technology to recognize what can happen to compromise the information they are trying to protect.

The NRC recognizes the importance of ensuring that users identify and understand the various threats that could result in serious damage to the systems, programs, and information they need to fulfill the NRC mission. The threat scenarios presented herein will enable them to recognize areas of vulnerability within their own computer environments.

The conclusions drawn from these threat scenarios are as follows:

- Although the possibility of outsiders gaining access to these systems does pose a risk, the risk that insiders could do damage is higher. The risk from insiders is higher because the physical controls at the various NRC sites restrict outsiders from entering the sites.

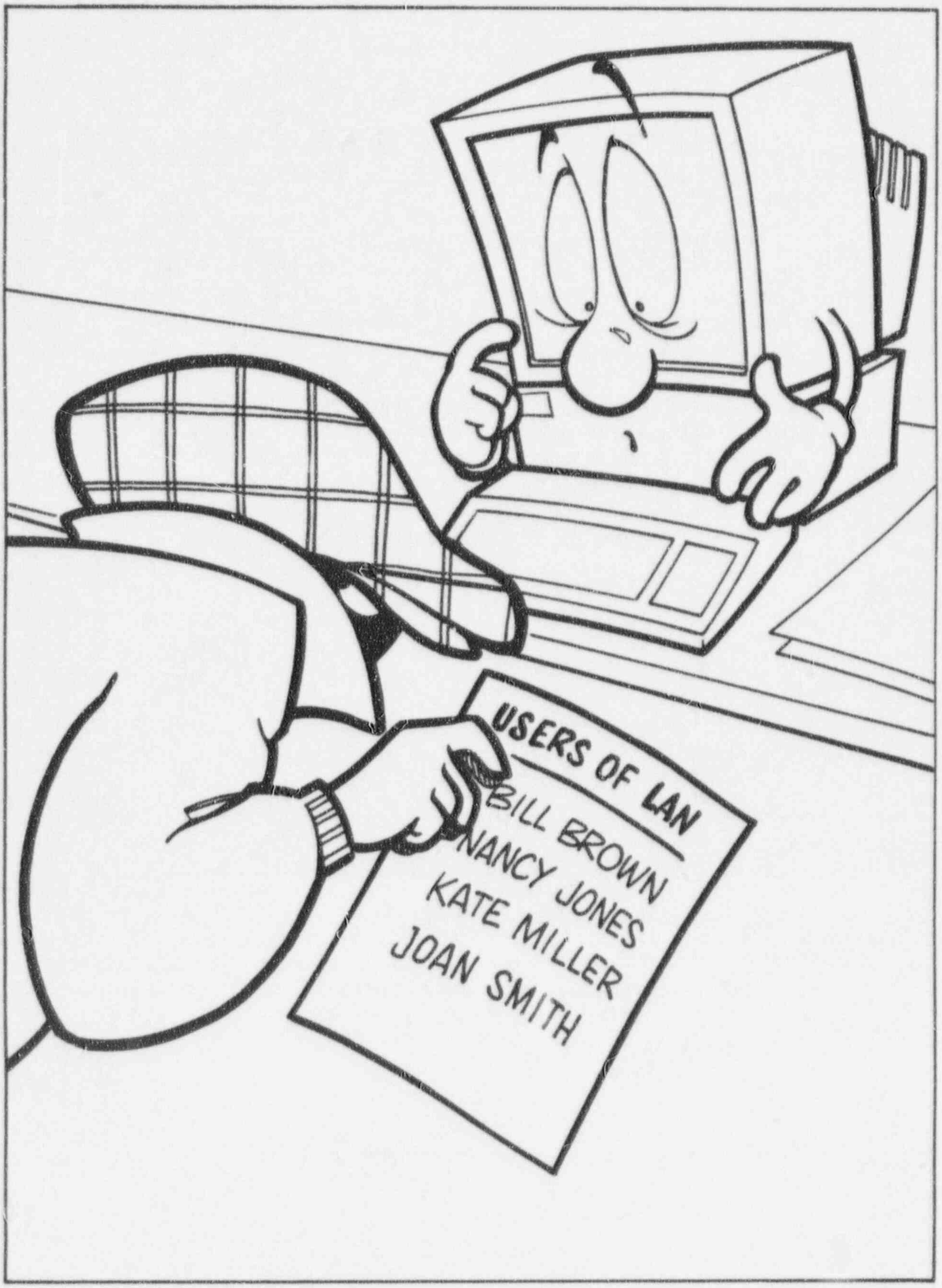
- The insider threat may not result from malicious intent, but more likely from errors in the use of security controls. These errors would most likely be caused in part by a lack of understanding of these controls. Eliminating errors in the use of security controls has become critical since most users are connected to the LAN.

Unauthorized access is caused by poor password choice

An intruder gained physical access to the LAN by using a microcomputer that did not have an access control mechanism (e.g., power-on password or access control software) and was connected to the LAN. The intruder was familiar with the names of certain employees who use this system. The intruder tried each name as a username and each birth date as a password. The intruder gained access to the LAN through a user account in which the user had chosen his birth date as a password.

Helpful Hint

NRC's LAN software requires users to change their passwords periodically. It does not, however, prevent users from using personal data for passwords. Therefore, users should avoid using easily guessed personal data for passwords.



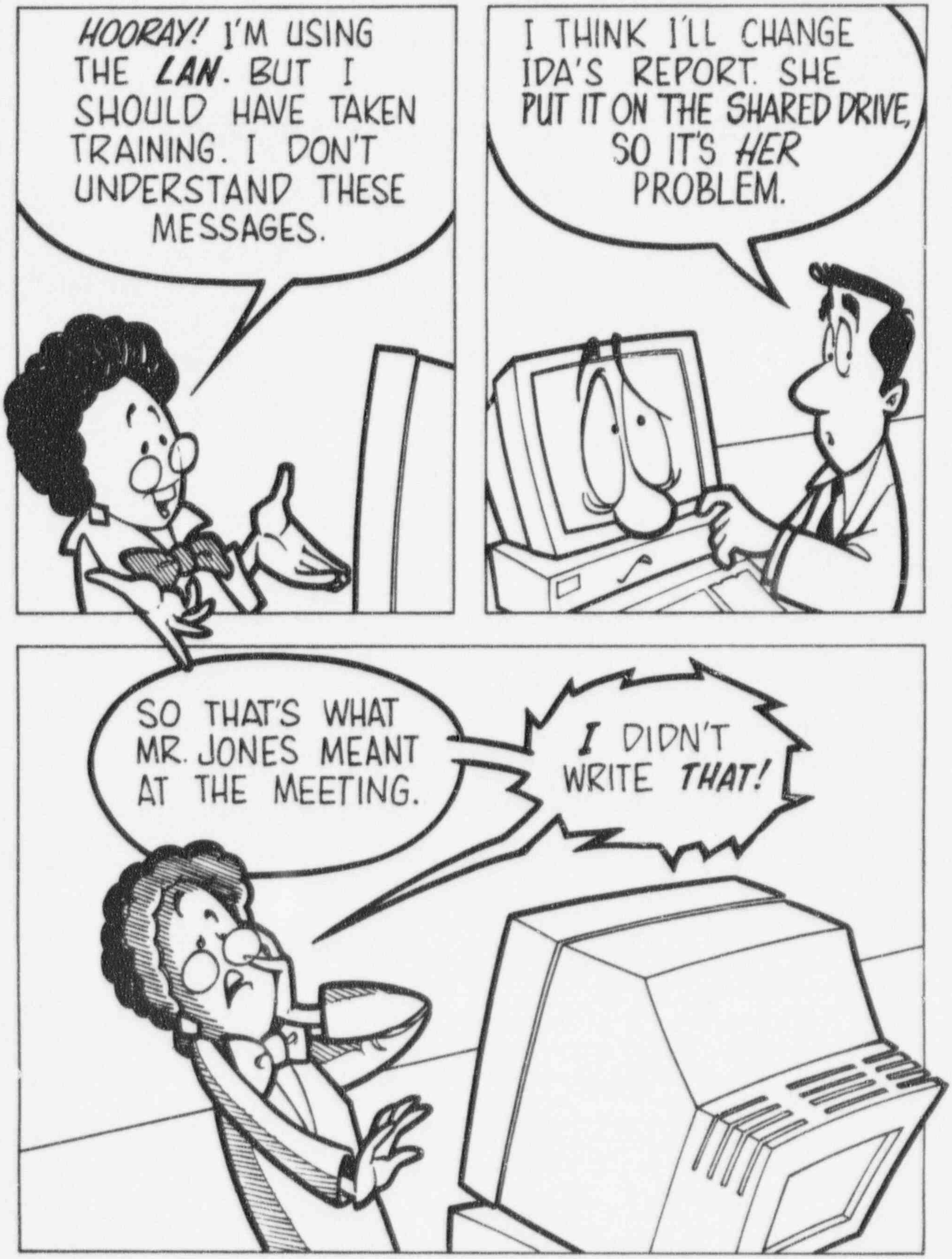
USERS OF LAN
BILL BROWN
NANCY JONES
KATE MILLER
JOAN SMITH

An unauthorized and undetected modification is made to a report

The manager was collaborating with other managers on a report. The report was to be released the next day. The managers were using the file-sharing feature of the LAN operating system and appreciated its benefits. However, none of them attended the recommended training classes and did not understand how the access control mechanism of the LAN worked. Each manager could access the file containing the report because it was stored on a shared network drive that all users of the server could access. Unfortunately, one of the staff members realized this and modified the report just before it was printed in final form and sent to higner management. The changes the staff member made were not complimentary to the managers.

Helpful Hint

Users of NRC's LANs can store files on network drives set up for individual, group, and server-wide use. However, the user is responsible for placing files on the appropriate drive(s).


HOORAY! I'M USING THE LAN. BUT I SHOULD HAVE TAKEN TRAINING. I DON'T UNDERSTAND THESE MESSAGES.
I THINK I'LL CHANGE IDA'S REPORT. SHE PUT IT ON THE SHARED DRIVE, SO IT'S HER PROBLEM.
SO THAT'S WHAT MR. JONES MEANT AT THE MEETING.
I DIDN'T WRITE THAT!

Electronic mail message is unauthorized

Most LAN users do not realize that electronic mail messages cannot always be trusted as genuine. A message that one manager received from another manager relayed a rumor of an impending major reorganization in which management positions might be eliminated. The manager who received the message fretted about this information but did not discuss it with the sender for one week. When the manager did discuss it with the sender, he learned that the sender did not know about the rumor and had never sent the message.

Helpful Hint

Before leaving your workstation, always log off, lock the keyboard, or use the Windows or other screen saver with a built-in password feature to prevent other people from waking up your screen to ensure that someone doesn't use your unattended workstation to "spoof" (make unauthorized use of your system to mislead a recipient) another user or send messages in your name.

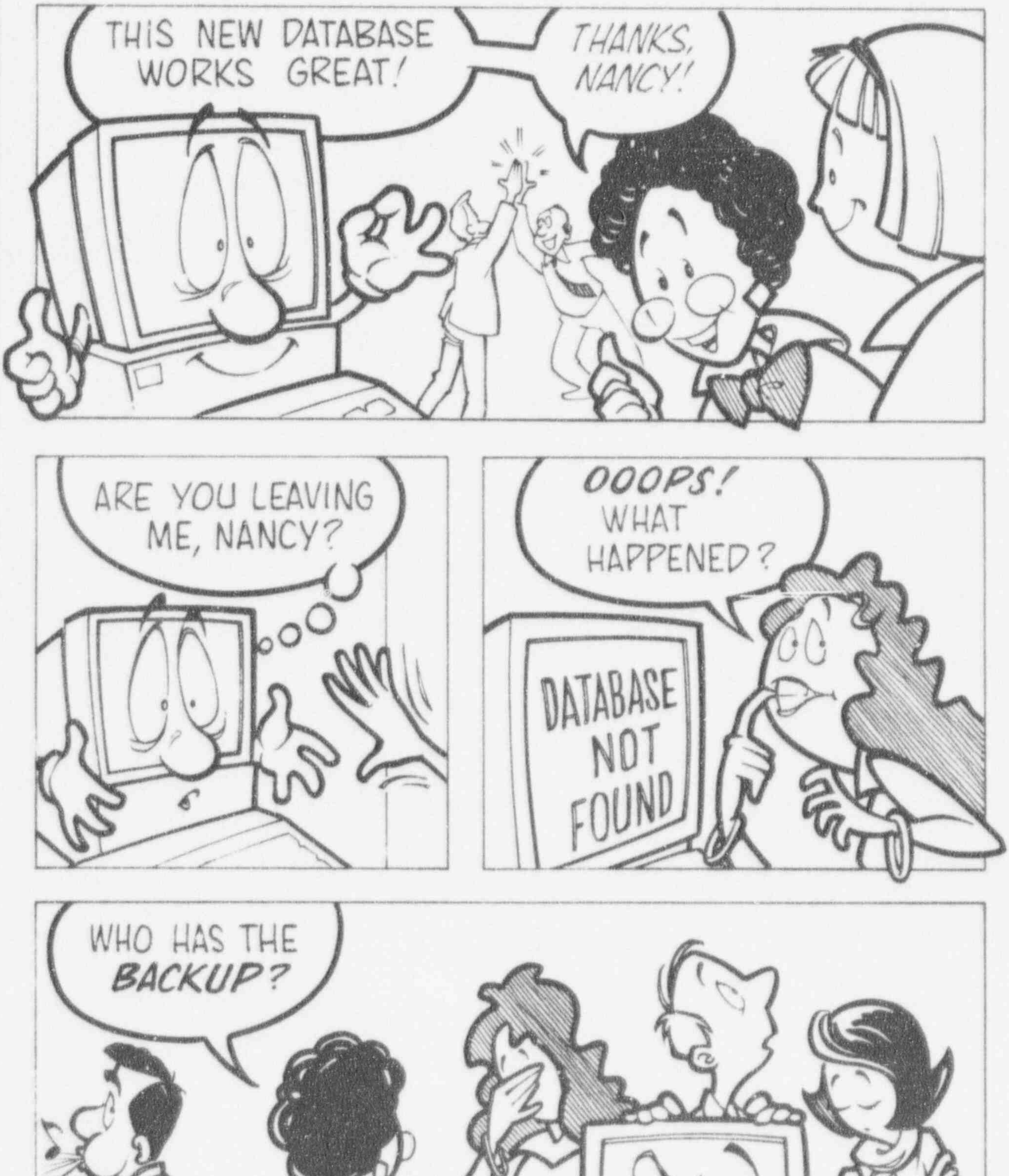
E-MAIL
E-MAIL

Processing capability is lost as a result of lack of application software backups

A working group purchased a new database package that allowed them to simultaneously create, modify, and access the information of the working group. The working group installed the database package in their shared directory on the LAN. The database software enabled the working group to make noticeable improvements in their productivity. When a new hire followed the instructions to access the database, he made an error and accidentally destroyed the database software. The user who had installed the database recently left the organization and took all her software with her. She mistakenly took the database software. No other member of the working group had made a backup copy of the software.

Helpful Hint

User organizations should remember to make and retain copies of software they acquire and support as well as data files.

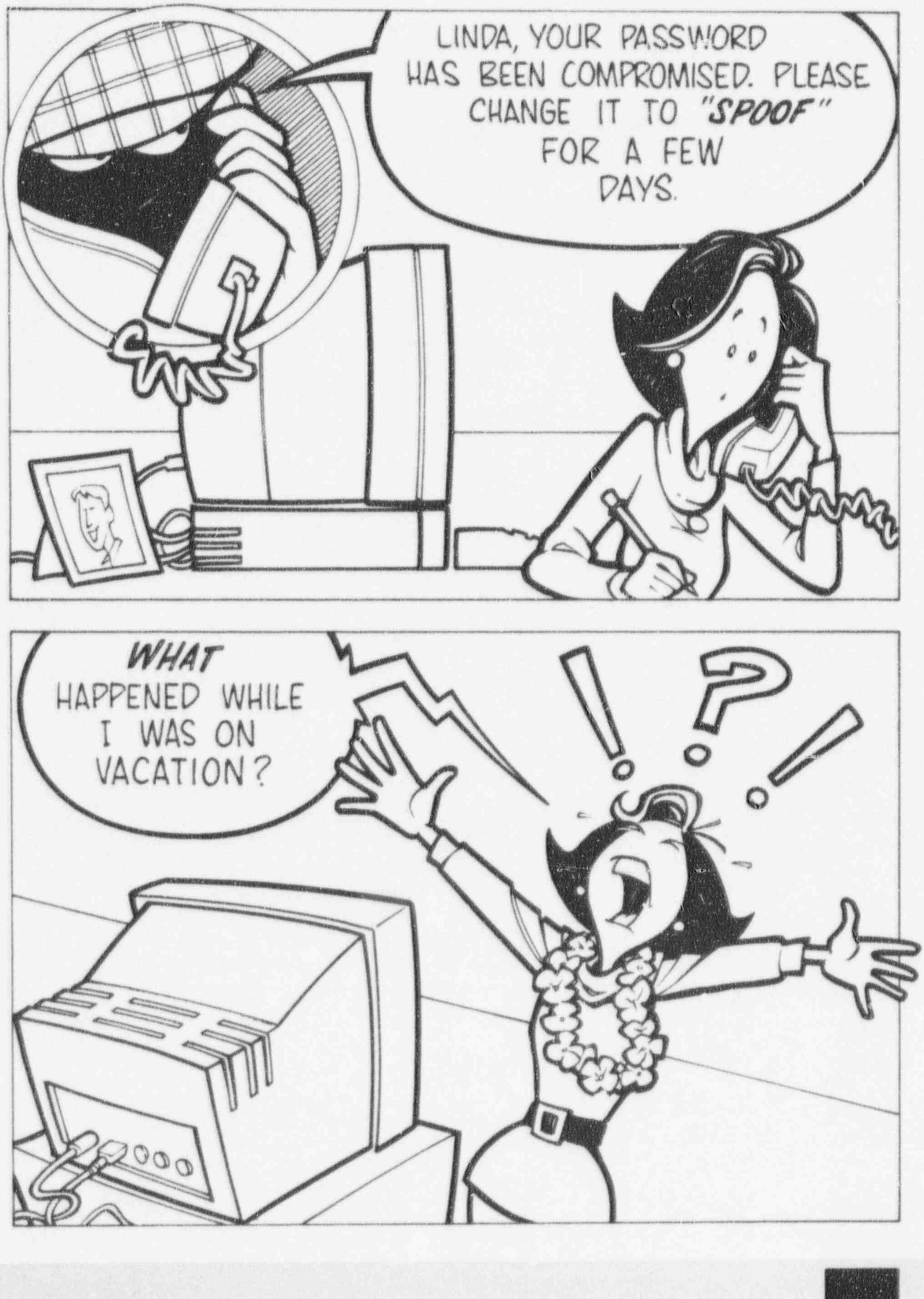

THIS NEW DATABASE WORKS GREAT!
THANKS, NANCY!
ARE YOU LEAVING ME, NANCY?
OOOPS! WHAT HAPPENED?
DATABASE NOT FOUND
WHO HAS THE *BACKUP*?

Intruders posing as LAN administrators lead users to compromise authentication information

A LAN user received a telephone call from someone claiming to be a LAN administrator. The *administrator* explained that there were problems with the authentication mechanism of the user's server and requested that the user change her password to *SPOOF*. The user was asked to log into the server using the new password so that the *administrator* could *monitor* the login session of the user from an *outside port*. The user did not realize that what the *administrator* was explaining was rather farfetched. The *administrator* asked the user to continue using the new password for a few days so that the *administrator* could continue *diagnostic work*. The server audit logs later revealed that sensitive files were accessed from the user's account during times the user was not in the office.

Helpful Hint

NRC LAN administrators do not need to ask users to change their passwords. Any such request should be immediately reported to the Office of Information Resources Management (IRM) Customer Support Center and NRC Computer Security.

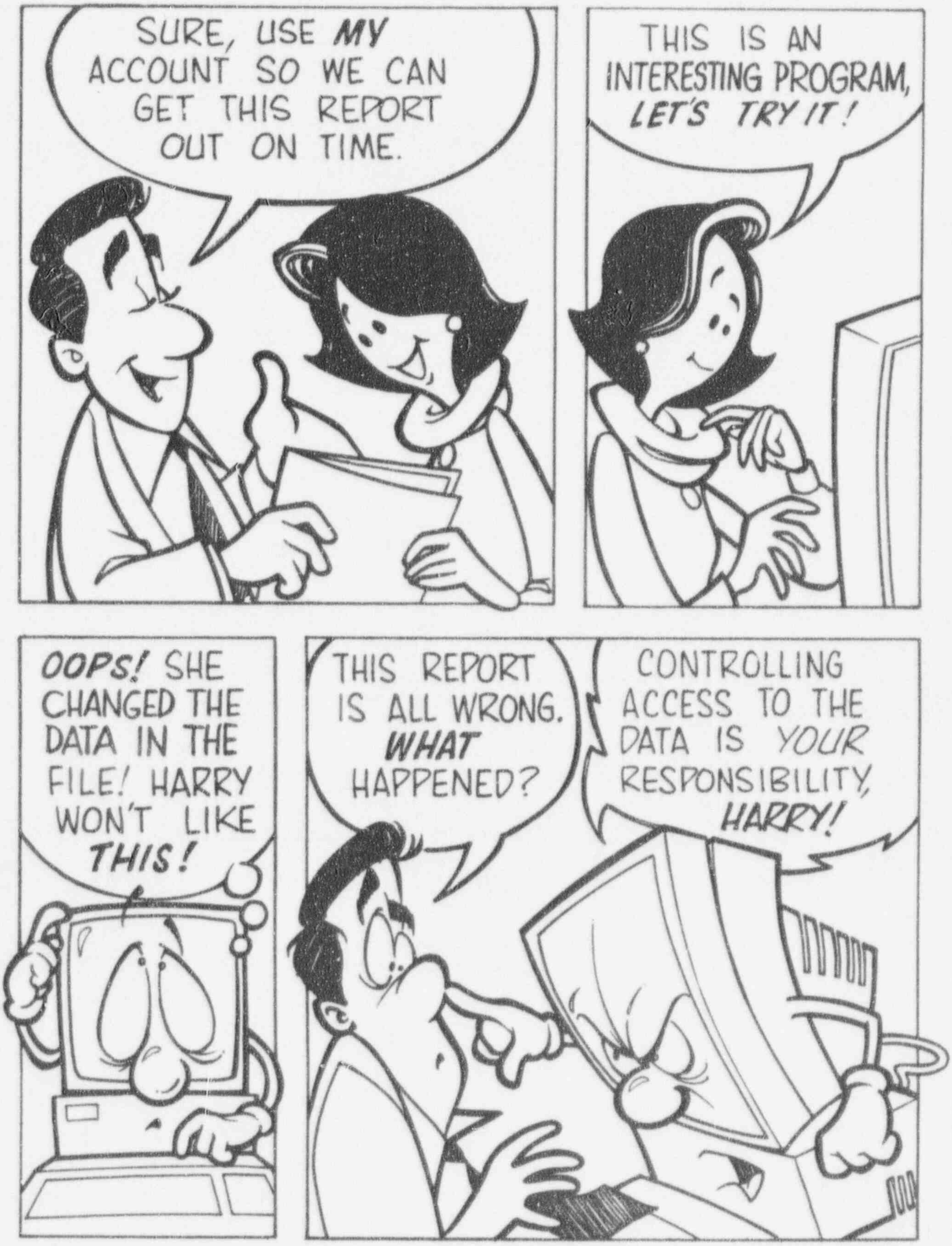

LINDA, YOUR PASSWORD HAS BEEN COMPROMISED. PLEASE CHANGE IT TO "*SPOOF*" FOR A FEW DAYS.
WHAT HAPPENED WHILE I WAS ON VACATION?
! ? !

Account sharing leads to unauthorized use

Two staff members were temporarily working on the same project and collaborating on a report. Each staff member was supposed to incorporate data from his or her primary areas of responsibility. One of these staff members was able to access, using his user account, more of the information needed to finish the report. The other staff member could not access this information, even temporarily, because of her other duties. To hasten the completion of the report, each staff member allowed the other to use his or her account. This agreement allowed both staff members to access all the information necessary to complete the report. However, one of the staff members was a curious system user and began to look at other files accessible from this user account. The curious system user also began to execute programs available to the other user. One of the programs that the curious user ran caused an update to be made of a file. Unfortunately, necessary backups were not done on the file in its previous state, and important information was lost.

Helpful Hint

Accounts should never be shared, even temporarily. Any problems that result are the sole responsibility of the account owner.

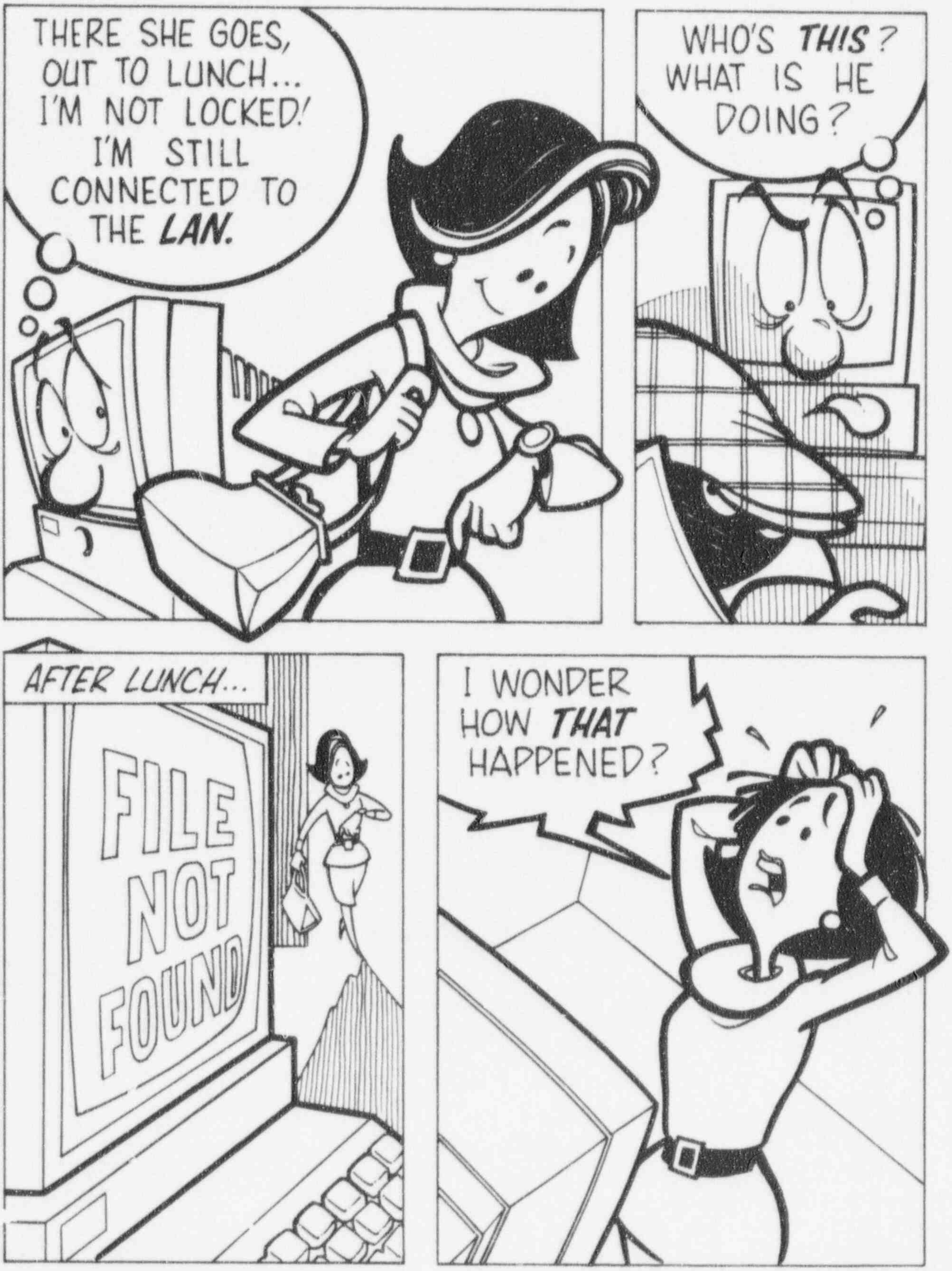

SURE, USE MY ACCOUNT SO WE CAN GET THIS REPORT OUT ON TIME.
THIS IS AN INTERESTING PROGRAM, LET'S TRY IT!
OOPS! SHE CHANGED THE DATA IN THE FILE! HARRY WON'T LIKE THIS!
THIS REPORT IS ALL WRONG. WHAT HAPPENED?
CONTROLLING ACCESS TO THE DATA IS YOUR RESPONSIBILITY, HARRY!

Unauthorized use results from unattended workstation

The audit log of a particular system showed that a specific user accessed a sensitive file at 12:30 p.m. on a Monday. At the noted time, the user was attending the retirement luncheon of a colleague. However, the audit log did not show that the user logged off the system to leave the area to attend the luncheon. An intruder used the unattended workstation and account to access the file. The user of the account was held responsible for the compromise of the file. The system also had to be reviewed to discover any other compromises that may have resulted from the intruder's access.

Helpful Hint

Before leaving your workstation, always log off, lock the keyboard, or use the Windows or other screen saver with a built-in password feature to prevent other people from waking up your screen to ensure that someone doesn't use your unattended workstation in an unauthorized manner.

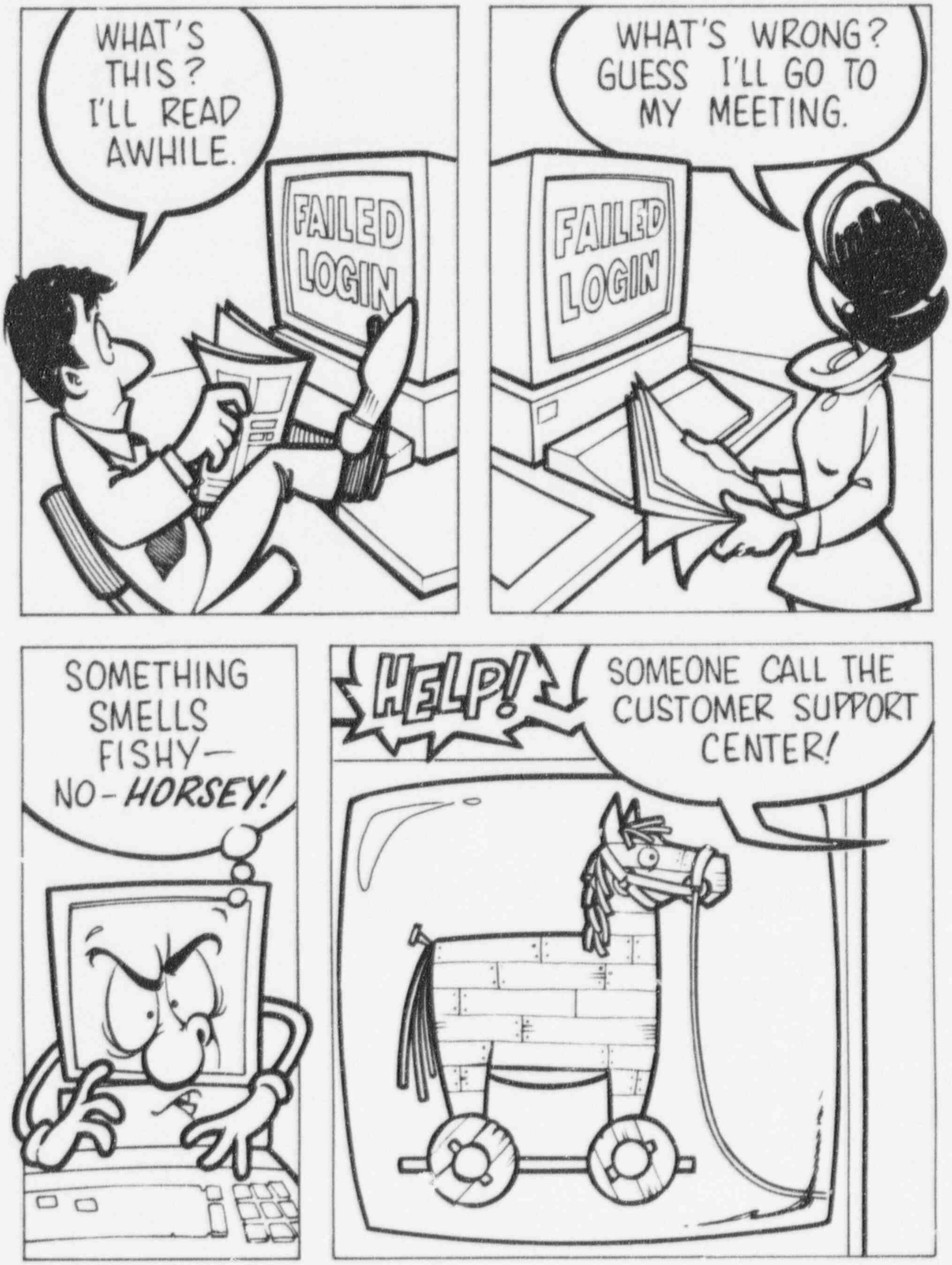

THERE SHE GOES, OUT TO LUNCH... I'M NOT LOCKED! I'M STILL CONNECTED TO THE *LAN.*
WHO'S *THIS*? WHAT IS HE DOING?
AFTER LUNCH...
FILE NOT FOUND
I WONDER HOW *THAT* HAPPENED?

Passwords are captured by spoofing the login sequence

One morning, each user of a particular system failed on his or her first attempt to log in. None of the users mentioned the failure to anyone else because failing a login occasionally is not unusual. The users did not realize that they were not using the legitimate login program executed by the operating system. Instead, the first (false) login screen was from a *trojan horse* program that merely prompted the user for username and password, recorded this information when typed by the user, issued a *failed login attempt* error message, and then allowed the legitimate login program to run, displaying the second (true) login screen.

Helpful Hint

Report suspicious or peculiar system behavior to the IRM Customer Support Center.

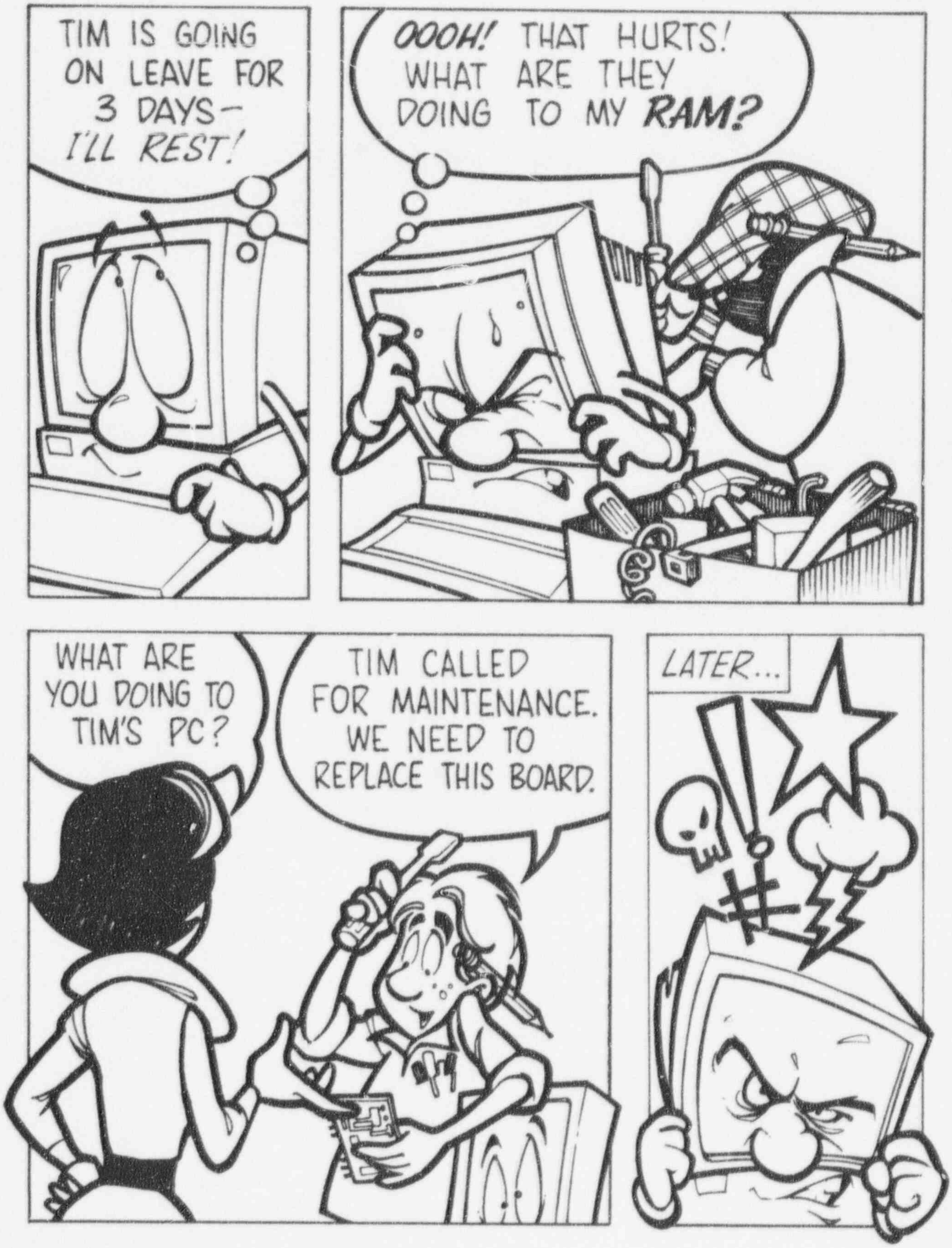

WHAT'S THIS? I'LL READ AWHILE.
FAILED LOGIN
WHAT'S WRONG? GUESS I'LL GO TO MY MEETING.
FAILED LOGIN
SOMETHING SMELLS FISHY— NO-*HORSEY!*
HELP!
SOMEONE CALL THE CUSTOMER SUPPORT CENTER!

An individual gains access posing as an authorized support person

Most of the office space in NRC buildings consists of open workstations, with the NRC employees separated by office partitions. A staff member in one of these areas had been using a word processing program to write a sensitive report. The staff member was to be out of the office for the next 3 days at a training workshop. While the staff member was away, an individual claiming to be an NRC microcomputer support person was questioned by NRC personnel working near the staff member who was away. However, the stranger convinced the other staff members that he was supposed to take the microcomputer out of the office for maintenance and would have it returned when the staff member finished his training. The other NRC employees allowed the microcomputer to be removed. The individual was never seen again, the computer was found in an empty office located in another building, and the information contained in the sensitive report was made public.

Helpful Hint

All NRC microcomputer support personnel have contractor badges and will display them upon request. When a technician reports to perform maintenance at a Headquarters location, he or she should present an IRM Customer Support Center ticket or similar request-for-service document. Most repairs to NRC microcomputers are made at the location of the computer and do not require the removal of the computer. Any variance should be reported to the IRM Customer Support Center. Also remember that files containing sensitive data should be kept on removable storage media (e.g., microdiskettes) which can be properly secured.

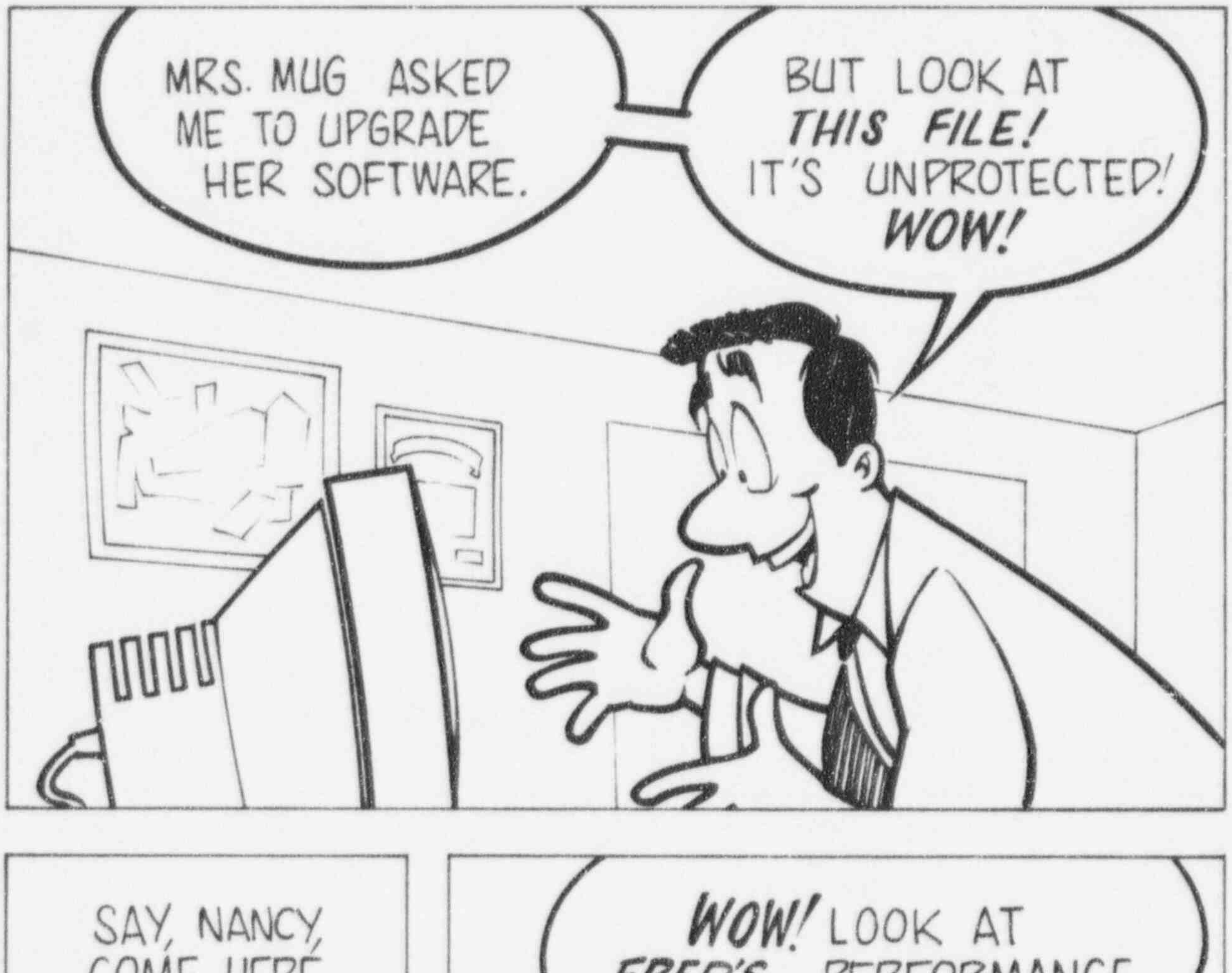

TIM IS GOING ON LEAVE FOR 3 DAYS— I'LL REST!
OOOH! THAT HURTS! WHAT ARE THEY DOING TO MY RAM?
WHAT ARE YOU DOING TO TIM'S PC?
TIM CALLED FOR MAINTENANCE. WE NEED TO REPLACE THIS BOARD.
LATER...

Information is compromised because of lack of file protection

A manager wrote the performance evaluations of staff members using the word processing software on a microcomputer. The manager had no protection on the microcomputer. A staff member who was installing an upgrade to the manager's microcomputer viewed the evaluations and informed the other staff members about what he learned concerning each of them.

Helpful Hint

Sensitive information such as performance evaluations should be protected by storing the data off line on diskettes or other removable storage media, using the password and file-locking functions of the word processing software, or encrypting the information.

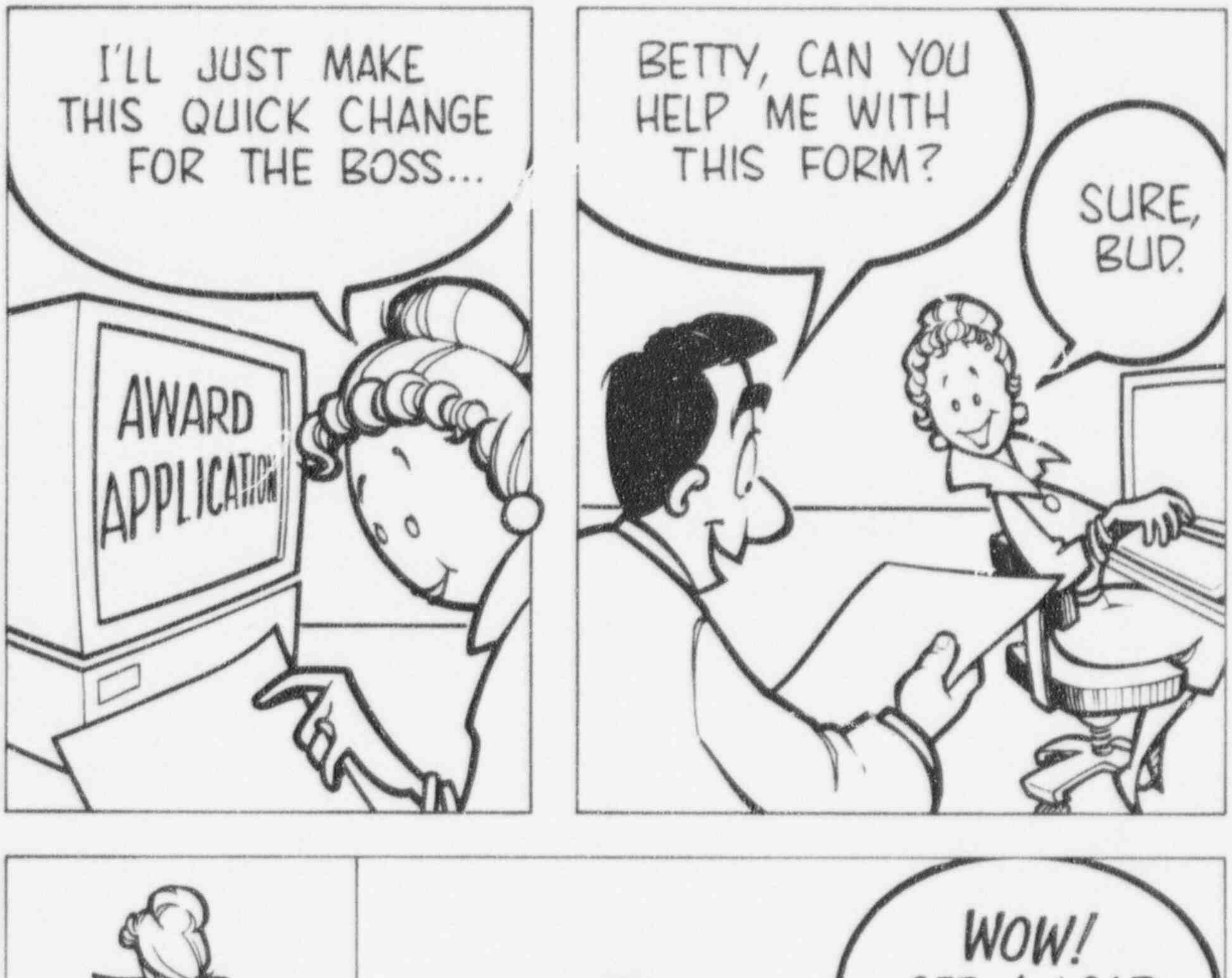

MRS. MUG ASKED ME TO UPGRADE HER SOFTWARE.
BUT LOOK AT *THIS FILE!* IT'S UNPROTECTED! *WOW!*
SAY, NANCY, COME HERE. I HAVE SOMETHING TO SHOW YOU!
WOW! LOOK AT *FRED'S* PERFORMANCE EVALUATION!

Compromise results from viewing monitor screens and paper output

An NRC manager was nominating one of her staff members for an award. She gave the application forms and justification memorandum to her secretary to integrate into a final package. While the secretary was editing the award application information on her microcomputer, another staff member entered the work area. While they were conversing, he glanced at the secretary's microcomputer monitor screen. The information on the screen was clearly visible because the screen was directly in the field of vision of anyone standing in the reception area of the secretary's office. The staff member noticed the award application, became upset about the nomination, and informed other staff members, who were also unhappy with the decision. The manager did not want this information relayed to the staff in such a manner. This situation could have been avoided if the secretary's monitor screen had not been visible from the high-traffic area.

Helpful Hint

Managers should work with the Office of Administration to ensure that sensitive information displayed on workstation screens is not readily visible to a passerby.


I'LL JUST MAKE THIS QUICK CHANGE FOR THE BOSS...
AWARD APPLICATION
BETTY, CAN YOU HELP ME WITH THIS FORM?
SURE, BUD.
WOW! GET A LOAD OF THIS!
AWARD APPLICATION

Unauthorized modification is made because of a lack of file protection

An NRC program reviewer prepared a report showing that an NRC program was not effective. The report was stored on the microcomputer of the program reviewer. The manager of that program thought that the report did not accurately reflect the results of the program and did not indicate possible positive outcomes. The program manager entered the office of the reviewer, opened the computer file containing the report, and changed the report to include more favorable comments about the program. The program reviewer printed a final copy of the report and not noticing the changes made by the program manager sent it to the appropriate people within NRC.

Helpful Hint

Sensitive information should be well protected by the information owner, or the person responsible for it. Options for protecting sensitive information include the physical protection of the machine (e.g., use of login passwords), physical protection of the disk or diskette used to store the information, use of the password and file-locking function of the word processing software, or use of encryption or other appropriate means.

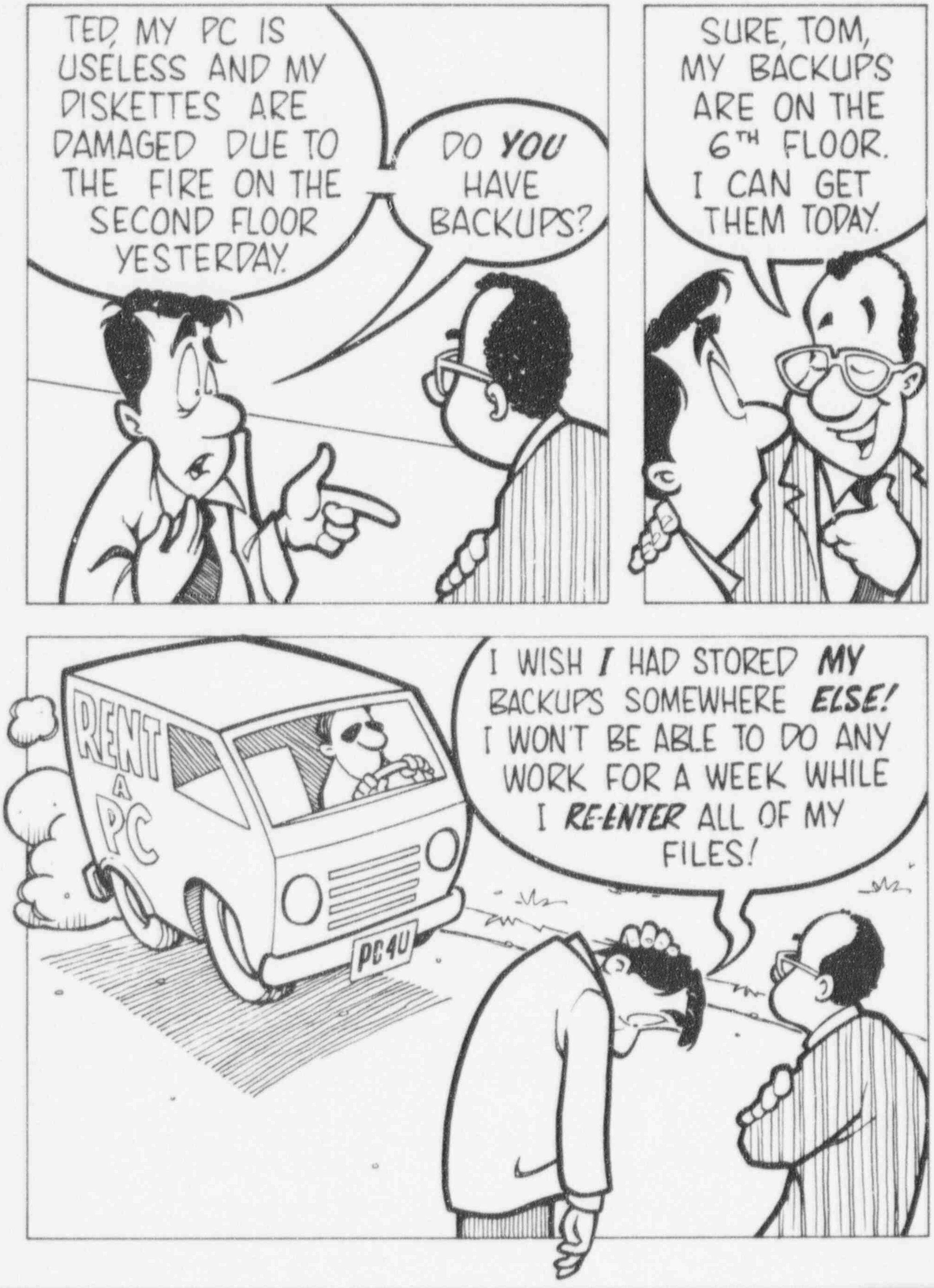
OH NO! JIM IS CHANGING THIS SENSITIVE FILE. I CAN'T STOP HIM...
AND HAL DID NOT PUT CONTROLS ON FILE ACCESS.

Functionality and data are lost because of a lack of contingency plans and proper backups

A fire in an NRC building caused damage to only one floor of the building. However, every floor sustained either smoke or water damage. NRC employees were allowed to enter the building during the initial cleanup process to get any time-critical documents or information. Unfortunately for most employees, the smoke and water damage made the microcomputers throughout the building unusable. This disaster greatly limited processing capability and forced employees to rely heavily on backups to reconstruct data and applications. Users who understood the importance of backups continued to work on microcomputers away from the site using backup copies of applications and data. Those who did not create backup copies, whether by lack of understanding or by conscious choice, could not quickly resume necessary and perhaps critical application processing.

Helpful Hint

Microcomputer users are responsible for backing up their own data and applications stored on their workstations and need to perform these backups at routine intervals. As a safety measure, it is useful to test that backup copies are actually usable. Documentation and backup media (e.g., disks, tapes) should be stored in a locked desk, file cabinet, or safe at an offsite location.


TED, MY PC IS USELESS AND MY DISKETTES ARE DAMAGED DUE TO THE FIRE ON THE SECOND FLOOR YESTERDAY.
DO *YOU* HAVE BACKUPS?
SURE, TOM, MY BACKUPS ARE ON THE 6TH FLOOR. I CAN GET THEM TODAY.
RENT A PC
PC4U
I WISH *I* HAD STORED *MY* BACKUPS SOMEWHERE *ELSE!* I WON'T BE ABLE TO DO ANY WORK FOR A WEEK WHILE I *RE-ENTER* ALL OF MY FILES!

Microcomputer functionality is lost because of damage from spilled liquids

An NRC employee was very proud of his horticultural achievements. He frequently brought various kinds of plants into his office and displayed them on his desk and bookshelves. His coworkers appreciated the plants, since they added to the office decor. However, the coworkers were not so understanding on the day he overwatered a plant sitting on the bookshelf above his microcomputer stand. The resultant serious water damage to his microcomputer forced the project group to use scarce funds to replace it.

Helpful Hint

Practice good housekeeping at all times, including not drinking or eating around your microcomputer. Most often, the damage that results from food and spilled liquid is inoperable keyboards and monitors. Users should realize that any such damage that results from food or spilled liquids is their responsibility.

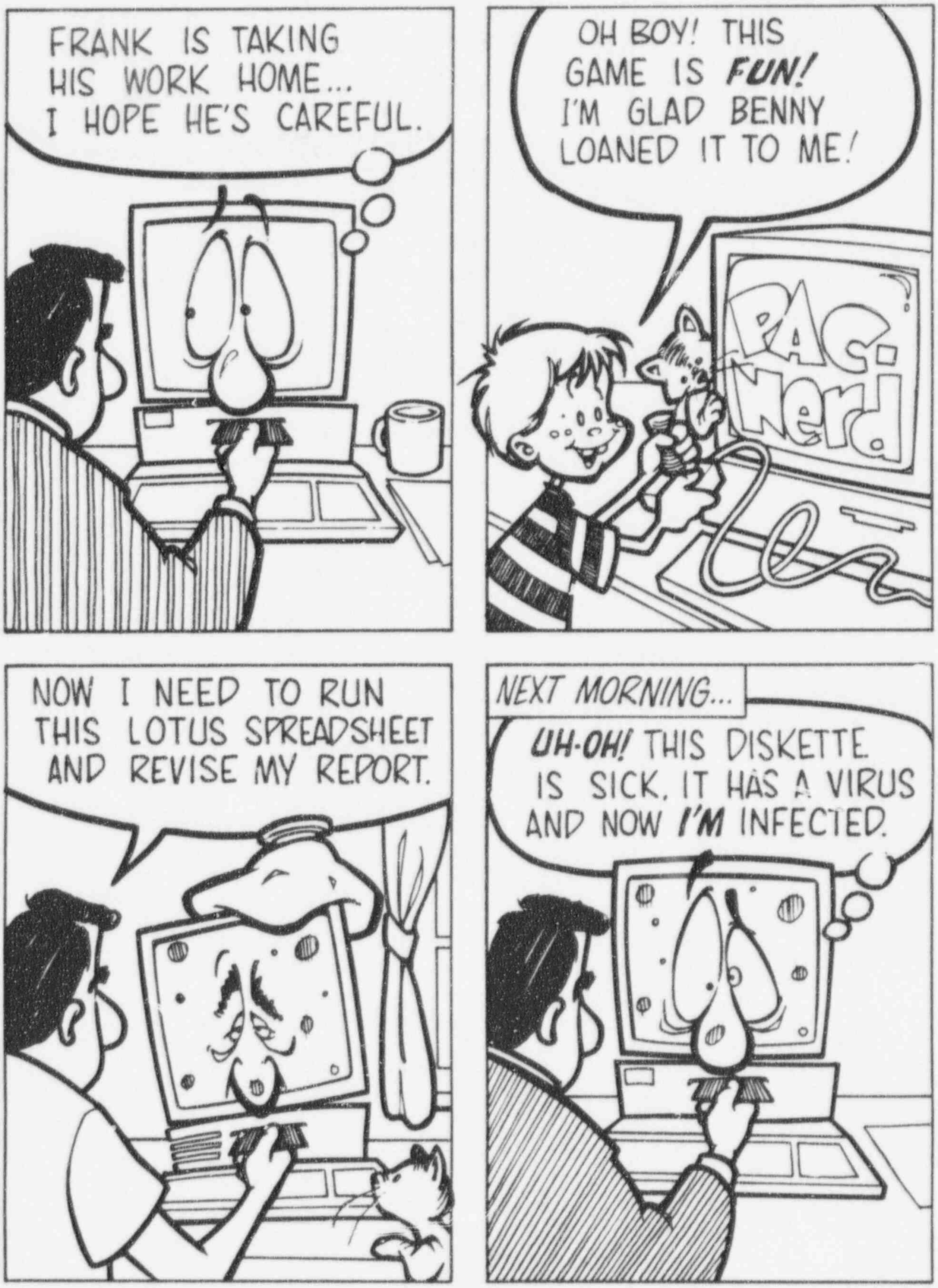
BLUB...
BLUB...
IM IN
TROUBLE...
OH NO!

Data and processing capability are lost because of a virus

A working group was collaborating on a statistical report. One working group member decided to work on the report at home. He took home a diskette containing a copy of the report and the statistical software needed to work on the report. He executed the statistical software on his microcomputer at home and worked on the report. Earlier in the day, the working group member's son loaded and executed some games obtained from a friend. One of the games contained a virus. The working group member's home microcomputer became infected. The working group member brought the statistical software back to work along with the report. The statistical software package carried the virus. He executed the statistical software on his microcomputer at work, infecting this microcomputer with the virus.

Helpful Hint

Never bring unauthorized or personal software to work. Beware of borrowed or unsolicited software. Check all diskettes obtained from either internal or external sources for viruses before using them on your workstation. Check computers used off site for virus infection before use. Virus-scanning software is available on the network. If you suspect your system may be infected, call the IRM Customer Support Center.

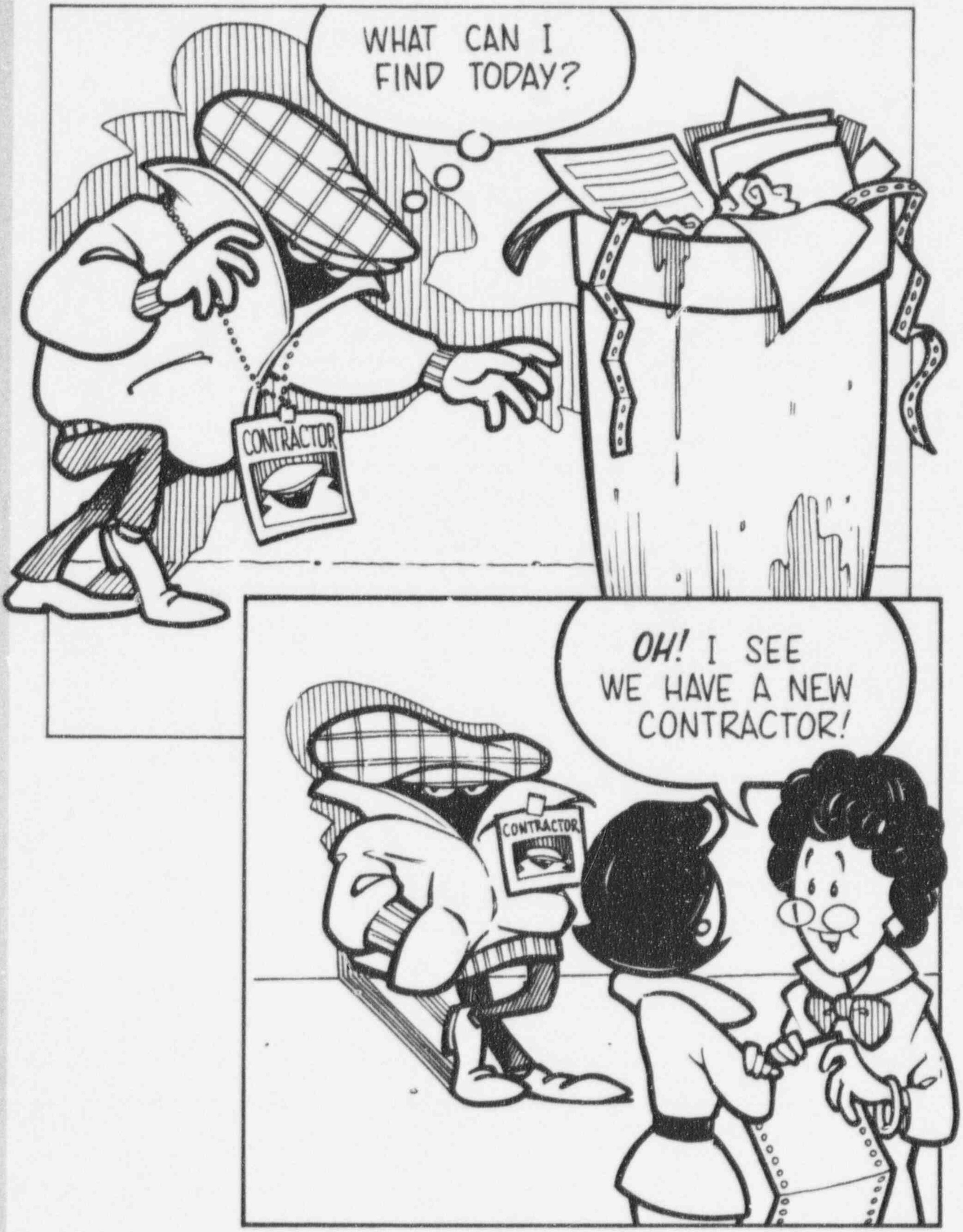

FRANK IS TAKING HIS WORK HOME... I HOPE HE'S CAREFUL.
OH BOY! THIS GAME IS FUN! I'M GLAD BENNY LOANED IT TO ME!
PAC-Nerd
NOW I NEED TO RUN THIS LOTUS SPREADSHEET AND REVISE MY REPORT.
NEXT MORNING...
UH-OH! THIS DISKETTE IS SICK. IT HAS A VIRUS AND NOW I'M INFECTED.

Stranger is present at a computer center or in an office environment

It is recommended that NRC employees question and, if necessary, challenge someone who is not generally recognized as an NRC employee or NRC contractor, but is in their office area or computing facility. A stranger wearing a contractor badge perused printouts placed in printout bins or trash cans. He wore a valid badge and thus was not challenged. However, the stranger had no official business in this office area or computing facility and was not authorized to be searching through printouts.

Helpful Hint

Always challenge individuals behaving suspiciously. Report any individual's suspicious behavior to the Division of Security (SEC). Dispose of documents and printouts containing sensitive unclassified information by placing them in receptacles designated for classified waste or receptacles approved by SEC for disposing of sensitive unclassified material.

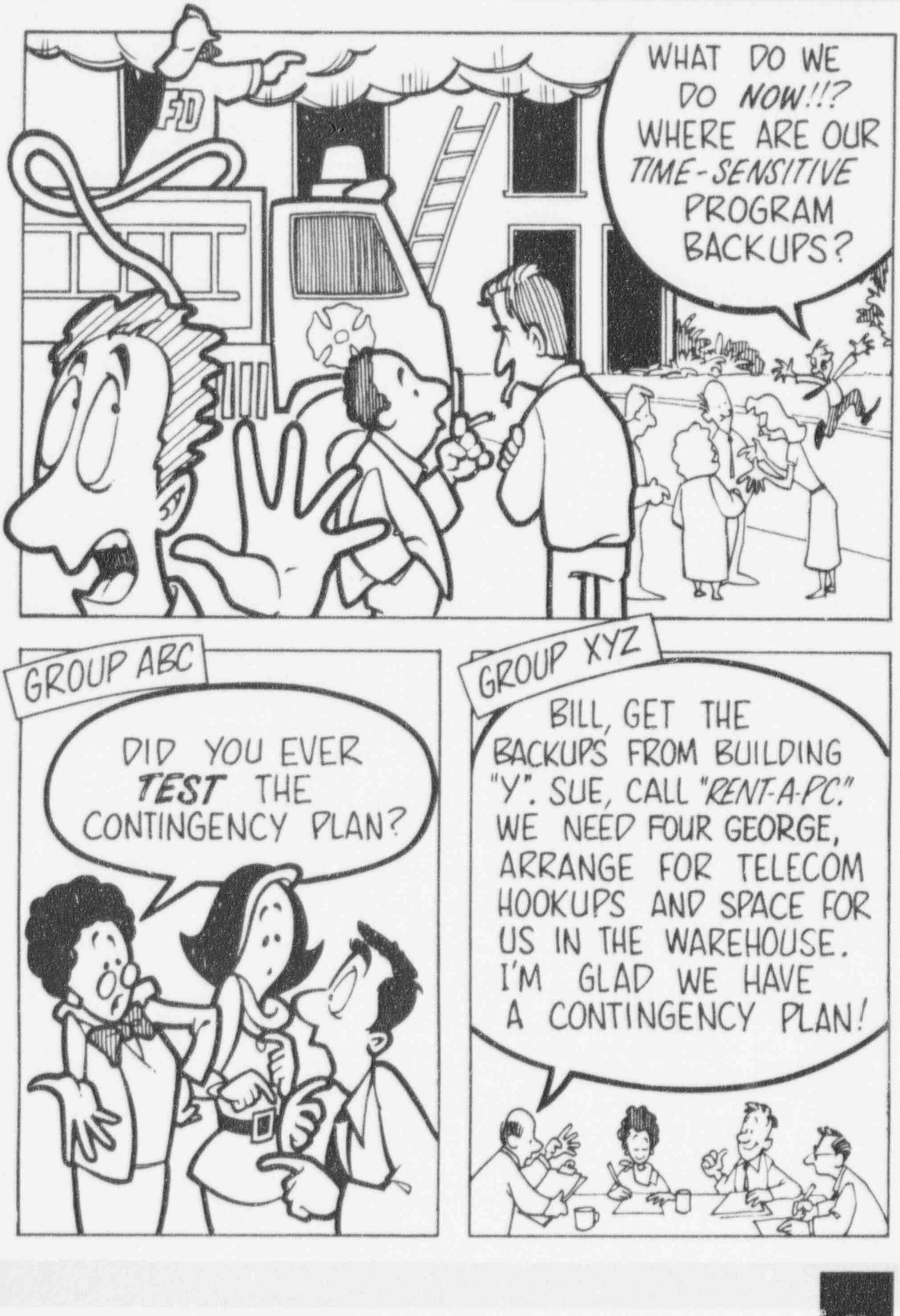

WHAT CAN I FIND TODAY?
CONTRACTOR
OH! I SEE WE HAVE A NEW CONTRACTOR!
CONTRACTOR

System services are not resumed because of lack of contingency and disaster recovery plans

A fire occurred in a building containing systems that process time-sensitive applications. Although the fire did not occur on the floors containing the computer systems, it rendered the building not structurally sound enough for employees to access the systems. Contingency plans and disaster recovery plans were implemented to ensure that the time-sensitive applications were running. Group XYZ information owners, system administrators, and users who had practiced drills using the contingency plans and disaster recovery plans returned their systems to operation in an acceptable period of time. However, group ABC information owners, system administrators, and users had never practiced drills in the use of the contingency plans cnd disaster recovery plans. They discovered the problems with their plans while trying to execute them. These employees did not get their time-critical applications running in an acceptable period of time. Some users even stated that they were not aware ot their system's contingency plans and disaster recovery plans.

Helpful Hint

Develop and test contingency and disaster recovery plans.


FD
WHAT DO WE DO *NOW!!?* WHERE ARE OUR *TIME-SENSITIVE* PROGRAM BACKUPS?
GROUP ABC
DID YOU EVER ***TEST*** THE CONTINGENCY PLAN?
GROUP XYZ
BILL, GET THE BACKUPS FROM BUILDING "Y". SUE, CALL *"RENT-A-PC."* WE NEED FOUR GEORGE, ARRANGE FOR TELECOM HOOKUPS AND SPACE FOR US IN THE WAREHOUSE. I'M GLAD WE HAVE A CONTINGENCY PLAN!

U.S. Nuclear Regulatory Commission

Office of Information
Resources Management

January 1996

NUREG/BR-0190