

November 15, 1978

## 'Tis The Season To Be Careful

### Pleasant Crowds Can Cause Losses

Despite cheerful music piped over the intercom and sparkling decorations dangling from the ceiling, the holidays are not always happy, or profitable, for department stores. The same hustling crowds that signal the season's arrival also can herald major losses, if dishonest employees utilize their opportunities.

After several holiday seasons of diminished profits, one department store employed several investigators to work undercover in various sections of the store. The investigators uncovered thousands of dollars in actual thefts as well as poor security.

One employee in the women's clothing department had a simple, yet effective method of stealing. With the help of a friend in the customer service department, she obtained "refunds" for items that had never been purchased. The clothing department clerk would write up a sales ticket and a refund approval for a non-employee friend who had not bought anything. The friend then took the approved refund slip to the confederate in customer service who approved the refund and paid the money. Later, the three would split the profits, usually on high cost items, such as coats.

Both employees were aided in their thefts by the pressure of the holiday crowds, which unfortunately caused store management to relax security policies. Refund slips were supposed to be approved by a supervisor, but the clothing employee (who had been hired temporarily for the season), was so seldom supervised, particularly during peak shopping times, that she simply filled out the tickets and was never questioned.

Holiday crowds aided another method of theft, one which investigators noted in several departments. The store utilized hand written sales tickets, with carbons, which were written out before the item was rung up on the cash register. The normal

procedure required an employee to write out the sales receipt, ring up the purchase, place the money in the cash register and give the customer a register receipt. The store itself circumvented this policy, with the intention of speeding up service. The results were numerous thefts.

Because of large crowds around a register in a particular department, employees were permitted to write up the sales ticket (which would suffice should the customer want a refund), hand the customer the purchase and then move toward the cash register and deposit the money and record the sale. Even if the customer did not have the exact purchase price, the clerk could make change while another clerk had the register drawer open, complete the transaction, and not record the sale on the register. Some employees did take the precaution of destroying the carbon from the sales ticket, although others did not bother, as the hand written tickets were seldom reconciled with register tapes. (Supervisors had "too much to do" for the next day.)

These losses and others of a similar nature largely stemmed from the store's eagerness to attract and please as many customers as possible. While this was no doubt achieved, loosening the store's normally stringent security procedures counteracted the potential for increased profits. Management needed to strengthen overall security. This could have included increasing security personnel at the store, placing more supervisory personnel on the floor and carefully checking backgrounds of temporary workers.

*As the holidays approach, store management should evaluate its existing security program to determine if additional safeguards are needed. Almost certainly, security should be tightened, not relaxed. Some additional hazards and suggestions are presented on the back page of the **The Lipman Report**.*

---

## Computer Security

### Do Not Bend, Fold or Assume Anything

*They send out bills and record payments. They streamline business operations, and they can cause more confusion than 100 untrained employees put together. Computers, the technological achievement of the 20th century, have the potential to cause catastrophic losses.*

*An estimated 150,000 commercial scale computers are in use in the United States today, and the number may double within the next 10 years. As the use of computers increases, so does the potential for increasingly devastating computer crimes. But, it is the human element that can cause or prevent these losses.*

*In the United States, estimates of current losses from computer-related crimes range from \$100 million to \$300 million annually. Some criminology experts believe, however, that less than 20 per cent of these crimes are detected or reported.*

*In a recent survey conducted by **The Gallagher Presidents' Report**, 100 presidents of large corporations were questioned about their computer security problems. Only about eight per cent indicated that they had incurred losses due to "breaks" in data processing security, and none of them attributed their losses to computer operator fraud.*

*In light of this, **The Lipman Report** offers this special report on computer crime. Its focus is primarily on the need for good internal security, because a dishonest employee can present the greatest threat to a computer system. This threat is compounded if management does not suspect its own employees, and has taken time to investigate them.*

Computer crime may be divided into four areas of vulnerability and they all have a common link — personnel security. Because computers depend upon the human beings who operate them, good personnel security, both before hiring and after employment, is vital. Personnel security is inadequate, both in public and private computer

operations, and this creates these vulnerabilities. Consideration of these potentially weak areas indicates the need for information about the people who work with computers.

The entry of false information into the computer system is one major area of vulnerability.

When the entry of false information is accidental, as was the programmer's error which caused 400,000 motorists in one state to be overcharged \$6 for their vehicle licenses, inconvenience is the primary result. However, when false information is entered intentionally, the potential exists for severe losses.

One such loss, of more than \$1 million, was incurred when an ambitious bank supervisor, a five year employee, abused his access to a computer terminal controlling customers' accounts. When crediting customer deposits to accounts, the supervisor altered records to reduce amounts of deposits and helped himself to the difference. If a customer complained of a shortage, the supervisor attributed it to a computer error, and corrected the amount in that account by diverting money from other accounts. His lucrative two years of computer theft ended, accidentally, when police raiding a gambling operation discovered betting receipts for one week that far exceeded his annual salary. Had the raid not occurred, the supervisor might have continued successfully manipulating computer entries indefinitely.

Closely tied to the entry of false information into a computer system is the unauthorized use of computer facilities, a problem which is created by poor security procedures. In this situation, the primary loss is caused by the theft of computer time even if no material items are stolen.

One seemingly innocuous example of unautho-

rized computer use occurred when some college students working part time in a campus computer center decided to use the university's multi-million dollar system to do their computer course homework, and also pass the long hours. The resourceful students used the computers to design calendars, pictures and interesting designs, which they subsequently distributed to friends. The students' entertainment was finally curtailed when they carelessly left some of their creative print-outs in the computer center, leading to an investigation by school officials.

A third type of computer vulnerability is the potential for alteration or destruction of information or files in the computer. This threat increases steadily as international terrorism grows, because corporations' and governments' dependence upon computers creates logical and effective targets. Restricting access to a few employees with high level security clearances is one preventative step.

In Italy, the Red Brigades and other terrorist groups have systematically attacked computer systems, both governmental and private. Such attacks could easily spread to other countries.

The fourth type of computer vulnerability is theft, electronic or otherwise, of money, property or data from a computer system. This could range from the removal of computer cards to the unauthorized withdrawal of funds by the previously mentioned bank supervisor.

Exposure to all four vulnerabilities — entry of false information, unauthorized access, alteration of information, and theft — can be greatly decreased by improving personnel security.

All employees should be thoroughly backgrounded to enable management to predict the integrity of employees, particularly those

employees who work in such sensitive areas. The problem of poor personnel security is due to the rapid advancement of technology, which has far exceeded the growth of security procedures. Employees involved in computer systems must be thoroughly investigated not only to determine any past dishonesty, but also to uncover any potential for committing dishonest acts once employed. This might include a history of gambling, drinking, or any other problem that could create a desperate need for money.

Laxity in this area is not limited to private companies. In one instance, the federal government was using convicts trained as computer programmers to operate programs involving large amounts of money. However, the government has established standards for computer hardware, in procedural, physical and personnel areas, and these standards are available to private companies.

Regardless of the level of technology, management must take the time and effort to investigate employees' backgrounds, verify references and exercise tighter supervision after employment to prevent devastating losses. Securing the system against outside attack is important, but protecting it against internal crime is crucial.

*The "computer age" has brought rapid advancement to business, and to society in general. Accompanying the advancement, however, is the potential for enormous losses carried out by illicit use of the computer. This illicit use can only be accomplished by people, but by learning everything possible about its employees, and closely supervising them, management can minimize its risks. A company would not install a computer without knowing how it operated; similarly, management needs information about its computer employees. That information could spell the difference between profits and losses for many companies using computers.*

---

## Holiday Problems

### Seasonal Thefts Drain Annual Profits

As the article on the front page indicates, the increased pressure of holiday crowds enhances the threat of losses to retail stores. A store whose security is inadequate during normal business operations could face serious trouble during peak times.

One potential problem arises from the seasonal need for temporary employees. These employees, frequently without prior work history may be hired quickly to meet the anticipated demand, before references and backgrounds can be checked.

Once employed, these temporary workers may not feel the same loyalty to the store as regular employees. They may also feel less accountable for their actions, because of their limited employment. These factors, coupled with additional pressures on regular employees and supervisors, can create a climate conducive to employee theft, if security procedures are not maintained and strengthened.

Of course, the increased pressure of holiday shoppers can also lead to a marked increase in shoplifting, and this is another reason to tighten security. However, dishonest employees have the potential to cause many types of serious losses.

The losses may occur in the form of fraudulent refund slips, which the employee prepares either for a friend or for personal benefit. Policies requiring supervisory approval of all refunds should be implemented throughout the year, and especially during busy times.

An obvious center of losses is the cash register, which, in busy departments, can be readily available to dishonest employees. Despite the crush of crowds, each purchase should be rung up on the register before the sales transaction is completed. This prevents employees from

pocketing the payment, or from giving away merchandise. Additional employees may wrap and prepare purchases to speed up the process, but money and purchase should not be exchanged until the cashier rings up the sale and gives the customer a register receipt. Supervisors should watch this procedure carefully to ensure that all purchases are recorded.

Another potential problem involving a busy cash register is the closing of the register drawer. The drawer should be closed after each transaction, and each transaction should be rung up separately. Not only does this require that sales be entered on the register, but it also curtails access to the cash drawer. If all sales are not rung up, and the drawer is frequently left open, it is easy for an employee to remove cash, or keep a customer's payment and it may be difficult to uncover a shortage later.

Supervision should be increased in all areas of the store, and procedures requiring reconciliation of cash with register tapes should be followed closely. Management also might consider increasing periodic inventories of departments and stockrooms.

*Holiday sales can be profitable times for merchants and can build a store's image. Tight security procedures can help ensure that the profits stay in the store, and that the only money employees take is their salaries.*



**The Lipman Report Editors**