

5.3 SECURITY AND LOSS-PREVENTION PROGRAMME

5.3.1 Overview

One study put the yearly loss from theft in US hospitals by employees and others at an estimated \$3000 per bed.

Another study suggests that 25% of all employees will steal to some extent if they feel that only a small percentage of the offenders are likely to be caught and punished.

The study further reveals that within that 25%, the management level culprit is responsible for over 60% of thefts.

Sometimes an employee who would not steal a rupee of hospital funds appropriates valuable articles of supplies for personal use.

Fraud and theft are a booming business in any society. Like corruption, they have become a global phenomenon.

They can strike from anywhere and often rear their ugly heads where they are least expected.

Figures relating to loss due to fraud and theft are incredibly high. Such figures are not easily available in India.

However, KPMG's India Fraud Survey identifies the sources of fraud as follows:

Employees 38%

Customers 19%

Service providers 15%

Suppliers 14%

Management 7%

Others 7%

Contrary to popular belief, it is not true that much of the losses due to fraud and theft is the handiwork of the lower categories of employees.

In fact, top management personnel engaged in embezzling can be more expensive and probably most difficult to detect.

Worse, it is not easy to punish them. Frequently, subordinates collude with their bosses.

Embezzlers are successful primarily because in most cases they are long-time, respected and trusted employees who handle cash, financial transactions and financial records or they are people placed in charge of purchase, store or similar functions.

Embezzlement is the most costly white-collar crime. Regular burglars and robbers do not do half as well.

In any organization, some employees are placed in certain strategic positions, which makes it easy for them to embezzle money.

The accounts clerks may maintain two sets of books, write cheques to fictitious names in the salary

register, give refunds to materials not returned, collude with suppliers in manipulating quotations and supplies.

Collusion, the cooperative meeting of two thieves, can be present anywhere in the facility.

It could involve a document falsification scheme between the employees of shipping and accounting departments; it could involve a major kickback operation between the purchase officer and the supplier.

Cheque forgery is said to be the largest single item of loss in the finance area.

Individuals with many opportunities to steal or commit fraud are officers and supervisors vested with authority, people with keys to sensitive areas, storekeepers, receiving clerks and purchase department staff, personnel handling cash, payments, payroll, financial and equipment records, employees on duty during evening and late night shifts, weekends and holidays, guards, long-time trusted employees and service departmental personnel.

Keys, time, lack of supervision and accountability, and authorized access to materials, money and records represent opportunities.

There is one other class of employees on which the top management should keep a close watch on.

These are the employees who linger at the workplace after regular working hours to complete "some unfinished business" or come back for work on Sundays and holidays for the same purpose even though they are not on duty.

One sensitive area of the hospital that warrants special attention is the purchase department, which is very vulnerable to fraud and kickbacks.

The management should be particularly wary of the purchase officer who is not interested in receiving competitive bids but prefers to deal with an established supplier.

The purchase officer's argument is that supplier is well known and the quality of his service and the prices are favourable.

This in fact is only a ploy to extend the kickback that the officer is receiving from the supplier.

Even if the prices are fair and the quality of goods satisfactory, this kind of an unchallenged long-term relationship always leads to many kinds of abuses.

Assured of business, the supplier becomes lax.

Orders may be neglected, top quality materials may be diverted to other organizations and poor quality goods will land in this hospital.

The purchasing officer with a vested interest will not complain of course.

Three elements – motive, opportunity, and means – are necessary to prompt someone to commit a criminal act.

The hospital management can effectively curtail only the elements of opportunity. The other two can only be constrained, not countered.

For example, the element of motive can be countered to some extent by preaching and practising a code of values, positive morale building, stressing loyalty to the institution and reminding employees of the consequences of theft and fraud.

The means may be curtailed by instituting internal control measures like unannounced audits, formulating well-defined policies for the control of materials, cash and other assets, checking and questioning all expense accounts, and so on.

Even then, employees are ingenious enough to devise new ways of committing fraud. The element of opportunity can and should be controlled.

The management has a moral obligation to safeguard the assets of the institution by making theft and fraud as difficult as possible, if not impossible.

Often, the general climate in the organization is such as to provide ample opportunity and temptation to the employees to indulge in fraudulent activities without anybody taking cognizance of those offences or punishing the offenders.

5.3.2 Internal Control

One of the primary responsibilities of CEO of any organization is to safeguard the assets of the institution against fraud, theft and other kinds of losses including waste.

However, the CEO and his to management team cannot exercise direct and personnel supervision overall employees and their activities – it is not desirable either.

They must depend on policies, regulations and a built-in system of internal control for the prevention of loss and for the efficient running of the organization.

Checks and balances are necessary in any kind of organization.

Internal control provides a built-in mechanism by which the work of one employee acts as a check on the work of another.

For example, the storekeeper does not have control on inventory records; persons handling cash do not have access to accounting records; the purchasing functions are segregated from the accounting and stores functions, and receiving functions from issuing functions.

Most hospital administrators believe in the folly of stationing a security guard at the main entrance of the hospital to monitor the members of the public who enter and leave the facility.

In prestigious corporate hospitals, the guards may be flashily dressed, making obeisance to VIP patients as they do in five star hotels.

Having done that the administrators sit back secure in the knowledge that all is well and that they have plugged the biggest potential leak in pilferage.

However, they fail to see the fertility of this exercise as long as they leave the employees' entrance and the shipping and receiving area open without any security check.

It is through those unsupervised passages that large-scale pilferage take place every day.

The amount of money lost through the front door over a 10-year period will in no way match the loss of the hospital suffers in one year through the back and service doors.

5.3.3 How the Hospital Suffers Loss

1. Embezzlement
2. Pilferage
3. Kickbacks and collusion
4. Equipment theft
5. Personal property theft
6. Payroll fraud and theft including fraud in purchasing the time clock.
7. Cash theft involving main cashier, subsidiary cashier(s), cafeteria cashier, etc.
8. Fraudulent practices in purchasing, receiving and storing
9. Fraud in registers, records, and billing
10. Computer fraud

5.3.4 Some Methods of Internal Control:

i) Physical Security

1. Guarding all means of ingress and egress. Protect the hospital against intrusion from without and illegal movement of goods from within.
2. Control of the hospital's perimeter. This is easy if the hospital is housed in a single building, but extremely difficult in sprawling campus-type layout with several buildings spread across a wide area.
3. Control of human traffic like employees, visitors, drivers, contractors, vendors, etc. conduct body search, if necessary.
4. Separate entry and exit points for
 - (a) Staff
 - (b) Patients and visitors
 - (c) Vendors, sales persons, delivery people and contractors.
5. Identify, scrutinize and guide the non-patient and non-visitors traffic such as vendors at the controlled gates.
6. Prohibit pedestrian traffic through unloading dock, receiving area, morgue exits and truck gates.
7. Control vehicles like delivery trucks, etc. and check outgoing vehicles.
8. Electronic surveillance of strategic and sensitive area through CCTV controlled or guarded gates

at all patient care areas.

9. Install locking devices and alarm system.
10. Issue visitor passes.
11. Procedure for and control over the issue of keys – master keys and sub-master keys. Authorization necessary to issue keys and an effective, enforceable procedure to retrieve them.
12. Lockers and lockable cabinets for staff against personal property theft.
13. Provision of a safe for patient's valuables.
14. Secured cabins for cashiers with a panic button or a silent foot or knee-operated hold-up alarm in their cabins.
15. Provide roll-up shutters or grills at strategic places for night time protection.

ii) Procedural Security

1. Establish service rules and communicate them to all employees. Each employee should be given a printed copy of service rules, the receipt of which he has to acknowledge.
2. Establish policies and procedure manual for each department.
3. Establish committees such as the general purchase committee, pharmacy and therapeutics committee, etc.
4. Establish accountability and control over the flow of hospital supplies and materials, particularly the receiving functions, and regulate the operation of receiving and unloading dock.
5. Institute inventory control procedures.
6. Establish well-formulated procedures for requisition, purchase indent, supply and distribution.
7. Do not allow the cashier to have both the keys to operate the cash register. The first key unlocks the mechanism for register operation and gives the total readings for money and number of transactions. The second key gives total either cashier-wise or by some other classification, and resets all totals back to zero. If the cashier has both keys, the prospects of fraud increase.
8. Institute a perpetual inventory system.
9. Conduct surprise checks of all departmental inventories.