

Issue # : SECOM/05/2007



Internal theft - the silent killer

Most customers tend to overlook the threats of internal theft within their organization. Internal theft can be defined as the dishonest act/s of the employee/outsourced workers/contractors/vendors/business partners resulting in a financial loss to the organization. Internal theft can be in any shapes or forms such as:



- theft of materials from raw, semi-finished to finished products at the customer's site - it can be on a small scale over a period of time or a single event resulting in a major loss
- accepting short delivery of raw materials and goods but signing for full delivery in cahoots with the vendor/s
- allowing for over delivery of goods against the delivery order or invoiced quantity
- documentation cheating - on delivery orders, service reports and invoices
- manipulation of accounts and company finances
- misuse of company assets e.g. company cars, petrol usage, etc
- petty cash claims and manipulation
- cheating on claims - traveling, OT claims, entertainment, medical, etc
- cheating on attendance and working overtime - on clocking in and clocking out
- selling of company secrets and information
- using competitors to bid against their employer for contracts

All the above involved an element of breach of trust on the part of the perpetrator/s. They have a criminal intend to cheat or take advantage of the company who entrusted them with certain responsibilities.

Internal theft can be controlled and prevented if the company takes strong counter measures. Internal theft is opportunity crime. Hence the strategy is to reduce the "opportunity" for the potential perpetrator/s. The following are some of the counter-measures a company can take to reduce the threats from internal theft:

Human Resource Policy

1. interview and recruitment
2. vetting process - reference checks, police vetting and substance offence
3. job rotation
4. check and balances
5. authority limit
6. whistle blower policy
7. Staff ID
8. Code of ethics

Administration

1. proper organization chart and work flow
2. clearly defined job description and authority limits
3. documentation flows and controls
4. proper management and supervision
5. signing authority for documents and cheque
6. Safe - to keep cheque, cash, important documents and files
7. Internal checks and balances
8. Proper contracts with vendors and enforce good code of ethics with business partners
9. regular audits
10. ISO compliance

Physical protection

1. perimeter fencing
2. proper lighting
3. building layout and internal partitions to restrict entry/movements e.g. server room, HR files, safe, store, etc

Security Protection

1. Security guards
2. CCTV
3. Alarm system with CMS and response
4. Access controls
5. Physical checks on people and vehicle movements in/out of the company premises