Loss Prevention

Proactive Strategy or Reactive Response?

Erik Kerten, (erikk@klpmaman.com) general manager of KLP Maman, is a former member of the Israeli ISA (parallel to the US Secret Service). During his service, Kerten held a wide variety of operational and management positions, including command of the Prime Minister's Protection team and units responsible for protecting Israeli and foreign dignitaries.

Mr. Kerten has a degree in Business Administration and considerable experience in managing security and civil projects. He is a Board of Directors member for several leading Israeli companies.

BUSINESS LOSS is a common phenomenon in the market and it significantly damages many companies' profitability. Against the backdrop of the current global recession where companies are experiencing financial hardships and trying to minimize expenses in any way possible, the question arises of whether companies are truly doing everything in their power to improve their profitability.

Loss prevention is actually an organisational perspective aimed at reducing or preventing potential losses. The approach suits any company or organisation that conducts some sort of operational or logistic business. The inventory, warehouses, movement of merchandise inside and outside the organisation, the interfaces between the various departments and the other processes and activities, are generally examined in purely operational and logistic terms of production efficiency and availability of logistic support and not through potential loss parameters. This may create a situation where the organisation loses a lot of money due to abuse or unintentional operational and logistical errors.

Loss prevention actions are meant to generate and implement work processes that completely integrate the inspection and security components with operations.

Minimising and/or preventing loss is a critical element in managing expenses and improving profitability. Loss minimisation is a long road strewn with surprises, since most organisations are not at all aware of the financial value of their annual losses (aside from inventory losses). Loss prevention examines all the processes within an organisation in order to find failures and weaknesses through which money can leak through the organisation.

The failure can be a breached process that can be exploited for theft or it can be a process that contains the potential for errors. The leak can appear in interfaces inside the organisation, in logistic or operational processes, and more.

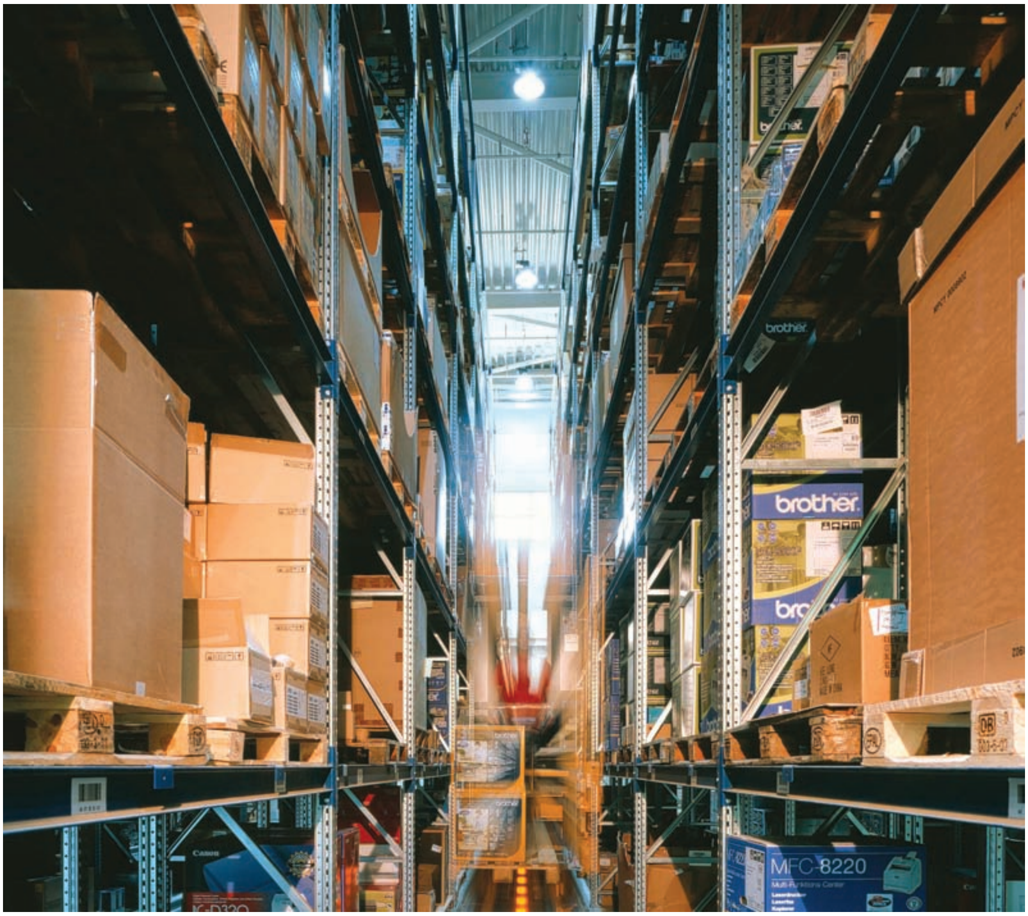
Loss prevention is part of the organisational strategy and not a specific reaction to an error or malfunction. The goal is to find the weaknesses and faults in an organisation and address them in order to eventually attain prevention on a daily level.

In most organisations, the company's problems are forecast to come from external sources and therefore, almost every company that takes operational efficiency seriously has a security officer that is responsible for protecting the company from external threats. However, according to a study conducted by the University of Florida, over 60 per cent of an organisation's losses are caused by internal factors that manifest according to the following:

System synchronisation – Bypasses and partial processes to the ERP systems that abuse the system, cause inaccuracies, and give options to alter operational procedures that help in cases of inefficiency, information leakage and abuse of the organisation's resources.

Destructions – Often, where a product is eliminated from the inventory and cannot be counted, a bypass is created where these products are reused but not through the company, causing the company to suffer twofold (eliminating useable inventory, reselling the product by someone else and thereby harming the company's sales).

Inventory management – "Closed" systems such as ERP systems do not enable changes to be made once the data has



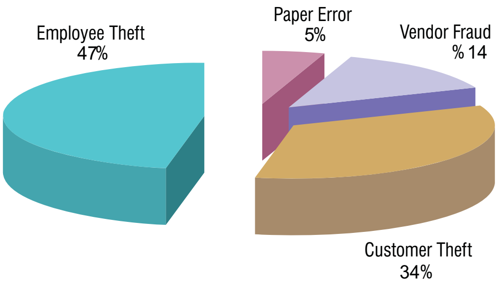
Source: DHL

The solution: *The main work perspective in the loss prevention process is preventative.*

already been entered. In many cases, data is incorrectly entered to the various systems, mainly due to typing errors.

Data verification – Two main problems in large organisations are data verification and control & inspection at the senior management level. In numerous cases, weaknesses in the processes cause a disparity between the actual data and the data on which operational decisions are made in the company. The majority of reports to senior management are made from middle management and from numerical reports, and decisions in the company are made based on the data that is received. These reports are often erroneous and there is a large disparity between the reports and reality.

Sources of Inventory Shrinkage



The main work perspective in the loss prevention process is preventative. Prevention begins when a weakness is identified in the organisation's operational / logistic activity. At the beginning of the process, we refer to three main types of loss: intentional, unintentional and hidden.

Unintentional loss refers to damage that is made innocently and unintentionally, such as an error in entering data.

Intentional loss refers to maliciously causing damage for various reasons such as revenge for dismissal, industrial espionage, etc.

Hidden loss is not considered loss but rather as an operational expense in an

> *"Loss prevention is part of the organisational strategy and not a specific reaction to an error or malfunction. The goal is to find the weaknesses and faults in an organisation and address them in order to eventually attain prevention on a daily level."*

organisation, such as prohibited use of organisational resources, which the pertinent entities are neither aware of nor have approved of.

Over 97 per cent of shrinkage is undetected by retailers at the time of the crime or subsequently. Over 31 billion dollars is lost yearly in the US alone to inventory shrinkage. This does not include 'silent losses'.

There are several options for working together with customers in loss prevention. Each way yields different outcomes and they can be combined in the work process:

Surveys – A survey that examines an organisation's status quo, main problems that cause intentional / unintentional / hidden losses in an organisation from a human resources perspective, the knowledge in an organisation, and the technologies implemented at the organisation. At the end of the survey, the organisation decides how it wishes to proceed (continue / discontinue business, independently fix faults).

The purpose of the survey is to increase the organisation's awareness and understand the sources of the faults that need to be addressed. As part of identifying the problems, the organisation promotes solutions, which lead directly to savings.

> *"Every manager, regardless of rank must ask himself at the end of each workday: How much money was lost today? Am I working to protect the company's profitability?"*

Work plan – An organisation that understands the conclusions of the survey and chooses to continue collaboration, undertakes a project where the survey is taken as a basis and every problem and flaw is analyzed and practical solutions are designed. Loss measures are specified during the project so the organisation obtains a status quo and move forward to measure losses.

Such a project provides the organisation with operational tools for solving problems, which directly lead to optimization, savings, and problem solving. The purpose of the work plan is not only to fix faults, but to initiate a process where the main motif is prevention as part of the organisation's routine, and not just investigation (which is based on one malfunction or another that is fixed, until the next one appears…)

Application – An organisation that continues to combine application is one that understands that loss prevention is part of its routine business. Thus, we will divide the application step in two – correcting faults and setting up a loss prevention entity / team in the organisation.

Control – Assisting the organisation's loss prevention team. The main profit component in this stage is a percentage of the savings.

Integrating the security layout in loss prevention – Utilising all the systems and personnel that work with security, for operations. Using security cameras to examine irregular processes that include theft and break in, and also ongoing checks of routine work methods to prevent malfunctions on a regular daily basis.

Using technology – Implementing specific loss prevention parameters in the organisation's current / future systems, such as WMS, SAP, and ERP.

Characterising and highlighting the irregular factor – Making the irregular element the only information received in reports and thus turning it into red flag that alerts every time a malfunction occurs. This makes focusing and efficiency in real time possible, while giving a solution, for example: an employee that does not arrive on time or a shipment that does not arrive at its destination.

In summary, loss prevention is gaining momentum in numerous organisations worldwide, and it has immense potential to save organisations a great deal of money and increase their profitability. However, there are still several factors that make it difficult for organisations to adopt this model, stemming from two main reasons: feeling intimidated and undermining the authority of the operations managers, the logistics managers and the security officers in an organisation, and the fear that middle and upper management have of their conduct in the company being criticised.

Loss prevention success results in savings, which significantly increases the company's profits. Every manager, regardless of rank must ask himself at the end of each workday: How much money was lost today? Am I working to protect the company's profitability?

Planned and controlled adoption of loss prevention measures may contribute to significantly reducing damages and will be financially worthwhile to the organisation. MG