Fraud, Theft and Organisational Loss: Threats to the organisation.
Bret Slade, Graduate School of Management La Trobe University.

I had the opportunity to travel interstate in April, and having some free time visited one of the nation’s better known retail electronics stores where it was my intent to purchase a new laptop computer to replace my daughter’s aging notebook.

Browsing the shelves I found a slightly shop-soiled Pentium IV laptop priced at a mere $850. Perfect! I gave the closest sales assistant an encouraging smile and beckoned him over.

“Wrap it up!” I said, “I’ll buy it.” I felt quite pleased with myself and knew that I would be in the good books with my daughter. However, as we often see, there can be a lot of ground to cover between intent and implementation, even in something as apparently simple as a cash transaction.

Struggling with the multiple levels of shelf-top security, the sales person found it necessary to call on the store manager for assistance in removing the item from its display. Some 35 minutes later I was still not in possession of the computer I was attempting to purchase.

The security on this item was not multi-layered; in fact it was mostly redundant. Securing the laptop to the display shelf was a Kensington combination lock and leash, an electronically alarmed parallel port connector, and a large black plastic pad adhered to the back of the screen, also leashed to the display shelf. Having time to watch the attempts to detach all of these items from the computer, I noted the following points of interest:

- The alarmed parallel port interface was removed with the use of a small screwdriver and rendered inert by switching off its power supply (time taken about 90 seconds);
• The adhesive pad was removed (subsequently damaging the computer) with a paint scraper (time taken about 15 seconds);

• The Kensington combination lock could not be removed as it seemed that no one in store had the correct sequence of numbers.

I would imagine the unit is still on the shelf today.

It seemed reasonable, while waiting for detachment of the item, that I express my curiosity regarding the nature of this security. I could understand the need to prevent walk-in-walk-out theft, but by any measure at least two of the anti-theft mechanisms were almost ineffective, whilst the third was restrictive to the point of inhibiting the sale of the item. The store manager’s reply astounded me. His view was that loss and shrinkage of laptops from the store was excessive and that even these measures were not controlling the problem.

My suggestion at this point was that an audit of delivery processes, access to the storeroom, the in-store stock control measures, rather than multiple security measures to the shelf space might be appropriate. By physical demonstration he had just proven that walk-in-walk out theft of these items from the shelf-top, without the use of screwdriver, wire and bolt cutters, was unlikely.

By way of anecdote this story alludes to organisational toxicity. Essentially, toxicity can manifest itself in any one or all four dimensions of employee theft, fraud, time-stealing, and employee harassment. It may be limited to one or a few employees, or it may involve many members. Ultimately, toxicity may be measured in the financial cost to the organisation and the psychological cost to individuals who must function in the work environment.

The effectiveness of control measures taken to eradicate toxic behaviours may depend on the identification of where and how these behaviours are taking place in the organisation. If stock is unlawfully removed from storage, used internally, finds itself
on the black market, or in the home of an employee, then this is theft. If it is inadequately controlled through poor accounting, stock-take and reconciliation measures then this may be attributed to human error. However, if these measures are exploited to hide stock loss, demonstrate non-existent profits, or financially benefit an employee, then this is fraud.

Any investigation of theft or fraud is rarely behaviourally focussed and inevitably takes place after a loss has been identified. In investigating loss, the classic investigator’s technique looks for the four factors of motive, method, means and opportunity. Let us take each in turn:

- Motive asks that the investigator look to see if the inducement to commit fraud, or theft, reasonably exceeds the perceived burden of discovery;

- Means asks the investigator to look for the “tools of the trade” necessary to open an organisational system to fraud or theft. This will include the possession of technical knowledge;

- The investigation of method seeks to identify how entry to the organisational system was achieved;

- Opportunity requires that a “moment in time” exists or existed to allow ingress into the system.

Ideally we would, as managers and members, like to see our organisations free of these behaviours. Of course, once fraud or theft has been discovered at any point in either the supply chain, or the organisational system, then measures come into place to identify and suppress these activities, external investigative bodies are involved, and it all becomes a matter of scale, financial cost and unpleasantness. Inevitably, the organisation hardens itself, places greater bars around its resources and it simply gets difficult to carry out the core business of the firm on a daily basis. As managers, we seek to invoke, support and spread behaviours that secure the organisation from internal toxicity. Behavioural change and the establishment of a “clean culture” is
very much the domain of the manager and in this the top down approach to management plays a large part.

A simple model describing the spectrum of activity and the prevention-suppression philosophy for the control of toxic activities may take the following shape (see Figure 1):

![Diagram of spectrum of activity and prevention-suppression philosophy]

Ideally, the preventative end of this spectrum forms the least costly part of the process of eradicating toxicity within the organisation. It allows for the establishment of a culture that is less vulnerable to the establishment of toxic activity.

At the far end of the spectrum suppression inevitably involves administrative, or lawful, sanction and processes that will ultimately involve the organisation in expensive legal activity. It also forms the basis for the delivery of a message regarding behaviour that is often as unpalatable to deliver as it may be to receive.

A strong preventative model will include a comprehensible code of conduct, clear lines of communication, appropriate induction and training, and the rewarding of positive behaviours that are essential to developing behaviours and attitudes that seek improve the organisational climate and culture. Ultimately, the organisation benefits by becoming a more efficient and effective competitor on the landscape, as valuable
resources are not wasted through the prosecution of employee infractions. An organisation prosecuting delinquent employees may suffer the combined dilemmas of financial cost, loss of public image, and damage to employee morale.

An issue that has not yet been addressed here is that of loss and shrinkage through the supply chain, particularly where multiple organisations are concerned. This is particularly relevant in a time where the outsourcing of non-core business functions is taking place. In this case, inter-organisational trust and a belief in the competence of partner organisations become critical factors. Organisations should be wary of surrendering the expertise to analyse externalised functions that are rendered on a fee for service basis, and should maintain their awareness that the greatest losses in the organisational supply chain may be found at the points of storage, transit and inter-organisational transfer.

Once again we are returned to the issues of inducement versus burden, and must ask why individuals are encouraged to act in ways that bring the organisation to activating sanction and suppressive measures. Far more disastrous is the situation that may occur when such behaviours are enacted by employees from different organisations linked in their activities in the supply chain. The scale and financial pain of the reaction when discovered is likely to be far greater, and has the potential to irrevocably damage inter-organisational relations.

Today’s competitive landscape is one on which the tempo of activity is continually increasing. Hyper-competition requires organisations to seek synergies with one another, often resulting in the outsourcing of important but non-core functions, or becoming strongly linked together within the supply chain. Efficiencies are sought by these organisations to enable them to deploy resources in the most effective fashion. Establishment of a climate of trust and a belief in competence, the reduction of employee delinquency and cultural toxicity within organisations is of increasing importance. This becomes more important as decision makers are made increasingly accountable for the performance of their employees, and their organisations as a whole. For today’s managers, cost saving preventative measures that seek to inoculate the organisation against toxic behaviours may play a greater part in
organisational structures and inter-organisational relations than expensive activities devoted to suppression and prosecution.

Acknowledgements:
Invaluable technical advice was provided to the author in the production of this article by:

Mr Andrew Barter MBA
Manager - Banking Fraud and Investigations Suncorp Metway Ltd

Major Michael Pemberton
Operations officer
1 Military Police Battalion