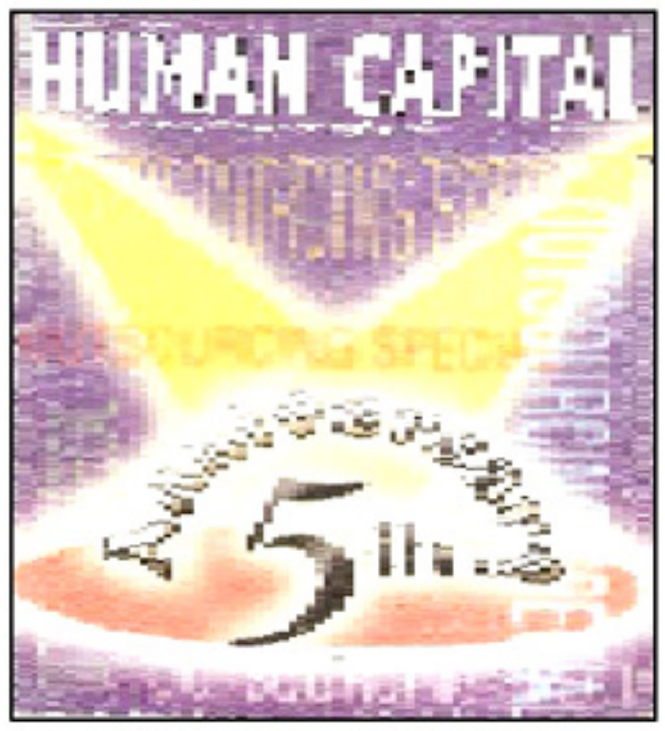
Trust busting



By R.S.Jagdev

It's a curious anomaly of the Indian business psyche that companies will spend crores of rupees computerizing their data storage, them put it all at risk for want of a Rs. 4,0900/- shredder.

It there's one sound that warms the heart of the security consultant, it's the hum of a paper shredder. These come spurting out of computers of corporate India.

Far too often, paper nuggets lie scattered around boardroom tables or tossed into rubbish bins. This carelessness has led to these printouts becoming the lingua franca, or common language, of corporate espionage and their best storeroom is a paper shredder.

FRAUDULENT CONDITIONS

As the economy starts to tighten, as it is now, accompanied by business confidence falling to a low point, fraud starts to increase. People who can't meet their car payments, mortgage payments turn to other methods to get cash. The solution is the company coffers. According to an international report of fraud, 65 percent of all respondents, including respondents from India, perceive fraud to be a major problem in their companies.

In hindsight it's often easy to identify the fraudulent employee. There are a number of red flags, Things like the staff member who's spending way beyond their means, too closely guards their interactions with vendors or suppliers, has personal, abuses drugs or alcohol, gambles, or never takes time off work.

As the economy starts to tighten, and business confidence falls, watch out for an increase of fraud.

FRIENDLY FRAUDSTERS

People think that fraud is a highly technical, space-age way of stealing money. Not so.

Anyone who can use a PC can get onto a system and milk it, usually by fiddling invoices, or putting ghost-employees on the payroll.

We can paint an incongruous picture of the average fraudster. They usually work very late, everyone loves them, they are president of the social club and organize all the functions such as the yearly party. They never take "sickies" and invariably have holidays banking up over the years. One day the unforeseeable happens and they are laid flat by a car accident or illness. An assistant opens the mail or accesses the database.

That's when the boss discovers why the staff member never took days off. What unravels is a trail of cash fiddling going back for years and mounting to tens-even hundreds-of thousands of rupees.

TOPPED BY TEMP

Look at one of our recent case studies. The staff member. - on this occasion a trusted female accounts person - was away for a week from her desk due to an illness in the family, which necessitated her going out of town for a period. What was discovered by her "temp" replacement was crude fraud in which the woman was diverting debtor's payments for her own use.

When called in by the company's auditors, we found a number of cheques that had been altered making the payee the woman's local furniture retailer. When interviewed we found that she had over 20 lacs in a credit account at the furniture company. Instead of taking the altered cheques to the bank to cash she was giving them to a source that was not scrutinizing the cheques. What is astounding is the fact that this offender had been fired from her last two bobs for similar frauds and had nine convictions for shoplifting. The company paid a recruitment agency good money for the privilege of hiring this person. The simplest of reference checks, credit checks, criminal history checks could have prevented this person being hired.

DATABASE DANGERS

At the other end of the scale is the highly sensitive area of company espionage. This, rarely, if ever, becomes public knowledge. Not only because of the embarrassment that often ensues but because it's very difficult to prove.

The computer was supposed to cr3ate the paperless office but the opposite is true. Where once the company's books were kept in a handful of ledgers and locked in a safe, now they're in a database that can be easily accessed by anyone with an access code. When printed out, these long printouts are often thrown into a rubbish bin. The trouble is that that's exactly where the corporate spy looks first. The opposition has been secretly clearing out your

rubbish skip for the past three weeks and now have the information they want-your quotes for 70 crore construction project.

BUG TALK

The prices of electronic bugging equipment have come down a lot from five years age. Now you can pick up a wireless microphone for under Rs. 5,000/- and have a boardroom meeting wired for sound. There is much talk about laser microphones and hi-tech speech vibration machines but the reality is that these pieces of equipment cost of fortune and are just not in abundant circulation in India.

The most ingenious of the bugs we found was in the company's boardroom contained within a videotape cassette. Placed alongside other nondescript videos, the item did not look out of place and the offender inside. We caught him eventually listening in to a walkman. It turned out that it actually wasn't a walkman; he admitted that he was just getting the inside drop on the other managers and staff.

Take the loss and move on?

How real is the economic espionage threat? According to the American Society of Industrial Security (ASIS), cases f espionage directed at international organizations have grown 260 percent since 1985. In the United States, the cost of this crime have been estimated at US $50 billion per annum. If you include the theft of intellectual property that figure soars to US $ 240 billion a year. Figures in respect of India are not available but they should be comparative.

Traditional protection options are just not working as deterrents to economic espionage. Corporate security systems often fail because they are set up essentially to protect people and physical assets not the ephemeral information flooding the world's new electronic highways.

Trusting that conventional resources will protect a company's trade secrets and operations from foreign espionage is out of date. If may actually border on managerial and fiscal irresponsibility.

An alarming number of companies seem to have resigned themselves to the boss of their trade secrets. This "take the loss and move on" approach is becoming increasingly unacceptable to shareholders, financial institutions, and insurance companies who must bear the losses.

INTELLIGENCE AND COUNTERINTELLIGENCE

There's no one, easy solution to countering economic espionage. However, there are way approach the problem, and they focus on top management involvement. Understanding the intelligence function and its role in modern economic warfare is essential to corporate survival. Countering economic espionage will increasingly demand that corporate leaders arm themselves with a working knowledge of intelligence and counter-intelligence. Then, they must equip their companies with business intelligence and counter-intelligence systems.

Economic espionage is the frontline of a new world economic war. It's a war that most companies from open, democratic, nations are ill-prepared to fight. An old business adage says, "Surprises end a career". Corporate leaders need to get up to speed, fast, on the grey people and grey areas of espionage.

Why not go and dust off that shredder today. HC

R. S. Jagdev is a private detective running Probe Intelligence Services. A former Personnel Manager, his practice concentrates on pre-employment screening and labour intelligence matters.