

Enterprise

www.telstra.com



More white-collar thieves taken to task

In the final article on fraud, **Mark Fenton-Jones** looks at how some companies are tackling the problem.

Businesses that once would have swept any incidence of fraud under the carpet out of fear of loss of reputation are now showing a greater willingness to deal with the bad guys. But they are still in the minority.

"Ten years ago the common reaction was that they did not want the publicity," forensic accounting partner at KPMG David Van Homrigh says.

He says more companies are prosecuting fraud and have implemented fraud policies telling staff that fraud will be reported to police. However, the willingness to pursue fraud does not represent a major about-turn by SMEs.

According to loss prevention company Pro Active Strategies, detected dishonesty by employees is estimated to be reported in as little as 3 per cent of cases.

Besides concern over bad publicity, SMEs also don't report alleged frauds because they lack confidence in the outcome of reporting to police or the prospect of a successful prosecution.

A consultant with risk management practice Business Risk International, Ron Robinson, is investigating frauds that range from a \$700 credit card scam up to \$270,000.

His job is to investigate the fraud, prepare statements and, if the client wants to take the matter to court, prepare the brief for under-resourced police.



An investment in security systems can pay dividends. Photo-illustration: KARL HILZINGER

KEY POINTS

- Employee dishonesty is reported in as little as 3 per cent of cases.
- Growing use of outside investigators to deal with fraud.
- Lack of confidence in the outcome of reporting to police.

"The police don't seem to take it as seriously as other crimes because there is no violence," Robinson says.

Anecdotal evidence points to a growing use of outside investigators to deal with increasing white-collar fraud that is often difficult to detect, especially when senior managers are involved.

But while managers have access to accounts and know how the systems work, detecting their fraudulent behaviour is not impossible.

Pro Active Strategies investigated the manager of a transport firm who was suspected of claiming fraudulent reimbursements for expenses he said were paid for by his personal credit card.

The investigation substantiated this suspicion and indicated that urgent action was required as his position afforded considerable access to and control over company funds.

His employment was terminated to reduce further risk of loss and to allow for more investigation to discover the true scope of the loss. His assets were traced and affidavits were prepared by investigators.

An application was made to and granted by the NSW Supreme Court to issue a Mareva injunction against the suspect.

The injunction prevented the ex-employee from disposing of about \$500,000 of his assets, while the full scope of the fraud was revealed to be more than \$600,000 of company funds.

Eventually the assets were transferred to the ownership of the company. The matter was then reported to NSW police for investigation. The situation does not have to reach the stage when police or investigators need to be called in if companies have strategies in place (see table this page).

And investments in systems can pay dividends beyond dealing with fraud.

When Queensland liquor retailer The Grape Group noticed a rise in both customer and employee theft, it increased its surveillance operations. Management had specialised fibre broadband carrier Uccomm install about 80 cameras in 30 stores.

The company's Fortitude Valley head office monitors the real-time video surveillance across the Uccomm network.

"We experience the highest number of thefts when staff are occupied at the point-of-sale terminal," The Grape's IT manager, Ivan Brebner, says.

"Our digital surveillance solutions enable staff to watch potential thieves on the screen of the point-of-sale device, without the thief's knowledge."

The digital surveillance systems resulted in a reduction of lost stock and had recorded annual savings of more than \$250,000.

fentonjones@afr.com.au

PROMOTING HONESTY

Here are the top 10 honest workplace strategies:

- Be clear on exactly what it is that the business considers to be honest and dishonest practices.
- Document the company's expectations and communicate these to all employees.
- Provide a variety of reporting mechanisms to ensure that there are no barriers to reporting by employees, and include one that is external and guarantees anonymity.
- Implement internal controls to manage the environment and make it easy to be honest and hard to be dishonest.
- Measure compliance to company procedures and correct breaches.
- Use business indicators to detect "red flags" that indicate dishonesty.
- Don't react emotionally when a dishonesty is discovered.
- Investigate fairly and consistently using professional investigators.
- Learn from incidents of dishonesty and make necessary changes to the environment.
- Talk to your employees openly and frequently about honesty incidents among staff and about employer expectations.

Source: Pro Active Strategies

Intellectual theft a growing problem for business

Mark Fenton-Jones

In the knowledge environment where information is a key to success, many businesses — and not just the small ones — fail to give sufficient attention to their most important resources, the human assets that walk out every night.

Fortunately for those businesses, most employees return the next day.

theft of intellectual property is a fast-growing one.

Melbourne-based retailer Michaels Camera-Video-Digital offers free training courses with all its products sold, and has established a training centre, supported by substantial manuals and literature.

In 2001, a competitor persuaded a manager at the training centre to leave Michaels and join them at their company as a trainer.

unlawfully taken training manuals, systems and literature and duplicated them at the new job.

An investigation by loss prevention company Pro Active Strategies

"We couldn't have a competitor blatantly and openly ripping us off."

The orders allowed investigators to conduct a search of the employee's private residence, the principal business of the new employer and the training centre.

An Anton Piller order is usually ordered by a judge if a company can establish a breach of copyright on intellectual property and a real risk that evidence pertaining to that breach could be destroyed by the other party.

as well as the manual itself which was the basic data," said Peter Michaels, in explaining the reason for taking the action. "We couldn't have a competitor blatantly and openly ripping us off."

Proceedings commenced in May 2001 in the Supreme Court of Victoria.

Under the terms of settlement the competitor acknowledged that the materials used in its courses