

***The average loss to business due to employee fraud and theft  
is  
\$9 per employee per day  
(\$2,000 per employee per annum)***

<b>December 2006</b> <i>A bank employee stole \$7.3 million from Bendigo Bank</i>	<b>December 2004</b> <i>A bookkeeper &amp; office assistant stole \$174,000 from her employer</i>	<b>August 2004</b> <i>A company secretary stole \$22 million from K&amp;S Corp</i>
<b>March 2004</b> <i>A payroll officer stole more than \$2.4 million from his employer</i>	<b>October 2003</b> <i>A bank manager stole \$19 million from the Commonwealth Bank</i>	<b>March 2003</b> <i>A financial company executive stole \$400,000 from his employer</i>
	<b>March 2001</b> <i>A female employee stole more than \$630,000 from an Australian law firm</i>	

A national organisation of fraud examiners estimates the average loss to business from employee fraud and theft at \$9 per employee per day. That amounts to about \$2,000 per employee each year. Employees steal in many ways. While some take money and property, other forms of employee theft may take more subtle forms such as wasting time, taking unauthorised time off, Internet surfing or even punching a time clock for another employee.

According to criminologist, Richard C. Hollinger, Ph.D., who directs the National Retail Security Survey, the results indicate that in 2002

***“..retailers lost 1.75% of their total annual sales to shrink, up from 1.69% the prior year.”***

Hollinger said that the results of the survey should serve as a wake-up call to the retail industry that shrinkage, and employee theft in particular, continues to be a multi-billion dollar source of revenue loss.

With the huge advancement in technology over recent years, data theft is the new 'invisible' crime and poses a real threat to all businesses. Because employees have access to vast amounts of data, any sensitive data is vulnerable in the hands of a dishonest employee. There are two main forms of data theft, the first with the intention of stealing someone's identity, and the second, the theft of information.

According to an article by the Sydney Morning Herald (18/2/2004), two-thirds of British professionals admit stealing commercially sensitive documents and data when they leave a company.

In a survey for *ibas*, a computer forensics specialist, it was found that among white-collar workers, 69.6% said they had taken some form of intellectual property from their employers

when they left. Email address books, sales proposals and presentations, customer databases and contact details were the most common kinds of data taken. *Ibas* said businesses might be losing commercially sensitive information worth billions of dollars.

***"It's happening in all businesses and through all levels of the company, from lower level admin staff right up to senior board level."***

Recent industry estimates indicate that nearly 80% of computer crime is committed by "insiders," at an estimated annual cost ranging from \$100 million to as much as \$1 billion.

***More than one-third of all companies declaring bankruptcy last year cited that they were "stolen out of business" by their employees.***

Employee surveys reflect the harsh realities of your applicant pool:

- 56% of working people admit they have lied to their supervisors
- 41% say they have falsified records
- 64% admit using the Internet for personal reasons during working hours
- 35% have stolen from their employers, by their own admission
- 31% abuse drugs or alcohol

Profiles [Step-One-Survey II](#) identifies and predicts problematic employee theft issues at all levels of the organization by pre screening prospective employees for patterns in behaviour. Additionally, Profiles Step One Survey II, a proven honesty and integrity test, helps companies find honest employees. It identifies job applicants that are honest, drug free, reliable, and hard working.

The Step-One-Survey II gives you critical information for making hiring decisions you won't regret.

If you would like to know more about the Step-One-Survey II as a recruitment screening tool to help you measure your candidates' work ethic, reliability, integrity and attitude to substance abuse, please email Mark Purbrick ([mark@profiles.net.au](mailto:mark@profiles.net.au))