

# Bosses byte back to protect secrets

If you're planning to desert your employer for a rival and take sensitive company information to sweeten the deal, it pays to know that in the world of forensic analysis, files are rarely permanently deleted and almost everything you do leaves a digital trail.

USB memory sticks and storage devices such as iPods, smartphones and portable hard drives have made the transfer and transport of digital

**From page 1**  
Paul Almond, employee and industrial relations specialist at law firm DibbsBarker.

It can happen in any company, but is most common in financial services and IT, where personal contacts and other data can lead to huge financial rewards. "Employees often have a belief that because they brought in a customer, that gives them an entitlement over the relationships — which, legally, is wrong," he says.

Warren Mallard, managing director of investigations and forensic company Lyonswood, has opened a forensic investigation division specifically to deal with an influx of workplace IP theft cases.

He says information "is being taken today in much more covert and devious ways than it ever was. Where once employees had to spend hours and hours to photocopy a stack of documents or photograph them, today they can use devices such as USB memory sticks to download a mass of data, or send it out by email". As employees become more tech-savvy, the methods they use to avoid detection grow more sophisticated. Take the case of a proud new father whose employer learned he was interviewing with a rival company at the same time as finalising a series of important tenders. His name cannot be revealed as the matter was settled out of court.

The employer — a Queensland company that manufactured equipment for the mining and telecommunications sectors — initiated stand-down and lock-down procedures: logging and archiving the employee's emails and preventing his computer from burning files onto CD or DVD. But

Departing workers are stealing electronic files, providing a security challenge to employers, writes **Alex Bossell**.

information easier than ever. But it's also easier to get caught. Companies in almost every industry now rely on complex computer

software, forensic and private investigators, and lawyers to protect their intellectual property from theft, or to nail the thieves once it has slipped through the net.

This can include anything from detailed client contact lists and financial and strategy data to tender applications and contracts.

More and more workers are taking files with them when they quit, says **Continued page 12**

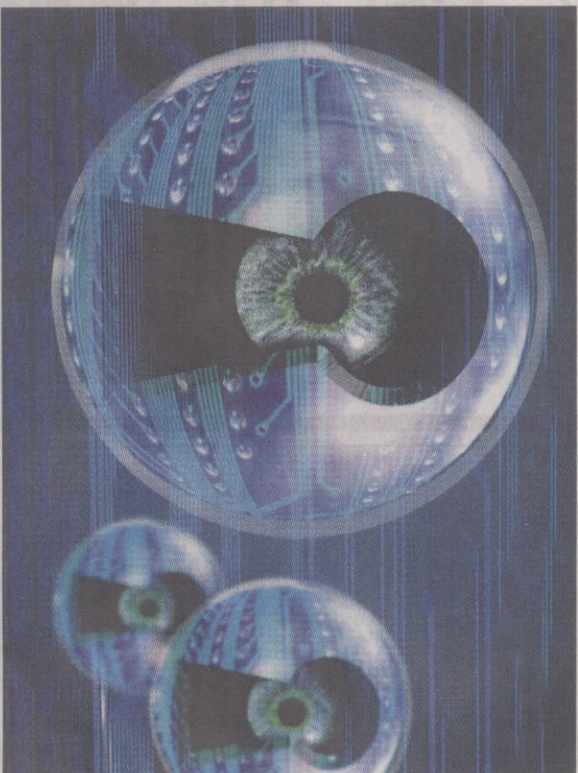


Illustration: KARL HILZINGER

**Even the tech-savvy are not immune to detection.** when the employee finally gave notice and his new company won the tenders, it was clear the lockdown had failed.

A forensic investigator, now working at corporate advisory firm McGrathNicol, was called and found that about 2000 files had been stolen. "This employee had recently had a baby and so every Monday he would bring in photos of the baby and show colleagues by plugging in his digital camera to do a little slide show," says McGrath partner Dawna Wright, who is familiar with the case. "After he had done the slide show he would delete the photos and download the files onto the camera."

Not only could the investigator retrieve details of every file that had

been taken, it could also determine the make and model of the camera, the photos that were deleted and details of the camera's memory card. Armed with this information, the tenders were reopened and the proud father was soon looking for a new job.

"A lot of the time, when the evidence is so strong, these things don't go all the way to court, because they know they are caught," Wright says. Aaron Dearden, employment law partner at firm Duncan Cotterill, says he suspects a lot of information is taken by employees when they accept new positions, but many employers do not have surveillance systems sophisticated enough to pick it up.

Dearden recommends employers

routinely run searches on a departed employee's computer for the terms "resume", "CV", or the name of their new employer or a recruitment company to check for suspicious emails or downloads.

"It's amazing the promises you will see that have been made. And the employer should say, 'If they have promised that, how is that employee going to deliver it if they no longer have access to our company's information?'" Dearden says.

"You then work backwards from the promise to see what documents they would have needed and check to see when those documents were accessed."

Other common tactics include setting up dummy email addresses to send fake correspondence to a wife or husband or attaching to emails important documents that have been renamed to appear innocuous. Experts say the smarter employees set up remote access to the company's main server from home, or take home hard copies over an extended period.

Lyonswood is investigating employees of advertising, photocopying and machinery supply companies, and has previously been hired by the NSW government to investigate employees of three departments.

"We have got two at the moment who have left their employers and completely wiped their computers of data. One of them, prior to leaving, had asked the information technology manager if he was allowed to put a USB device on his computer for a totally different reason," Mallard says.

"We're now data mining that computer hard drive so we can forensically acquire that data and any data

he transferred onto that memory stick."

Lyonswood also uses private detectives to follow a suspected employee, particularly if their employer is tipped off by a security company that someone is regularly gaining access after hours.

Freehills employee relations partner John Cooper says technology can both help and hinder employers in their bid to protect their property.

"There is no doubt that a variety of different technologies make it easier for people to remove employers' information," Cooper says. "On the other hand, technology assists the employer to prove its removal. The problem is, it all happens pretty quickly and the damage might be done before you can get to court."

Employers can use legal instruments known as Anton Pillar and Mareva orders to try to limit damage after the removal of information. An Anton Pillar order permits lawyers to search for assets and documents removed from the company. A Mareva order freezes assets of the employee to prevent their disposal before a trial.

"These are orders that can be sought urgently, often at the time the removal is detected and well before a final trial of the issues takes place," Cooper says. "As such they are very effective and powerful in recovering information that has been removed."

Employees, and their new employers if they participated knowingly, could face proceedings for breach of employment contracts, confidentiality provisions, theft, and obtaining a financial advantage by deception. The penalties are large but so are the potential rewards.