

PROTECT YOUR COMPANY'S INTELLECTUAL PROPERTY

Trade secrets, databases and systems are valuable assets that are highly vulnerable to misuse. *TradeSmart* outlines a comprehensive IP protection strategy. By Julia Nekich

The term intellectual property (IP) often brings to mind registered trademarks, copyrighted material, industrial designs and patents. All are protected by legislation and case law that defines and protects the owner of the IP.

But how does a business protect its confidential information, trade secrets, databases processes or systems – particularly when staff leave, or when business functions are outsourced to third-party suppliers?

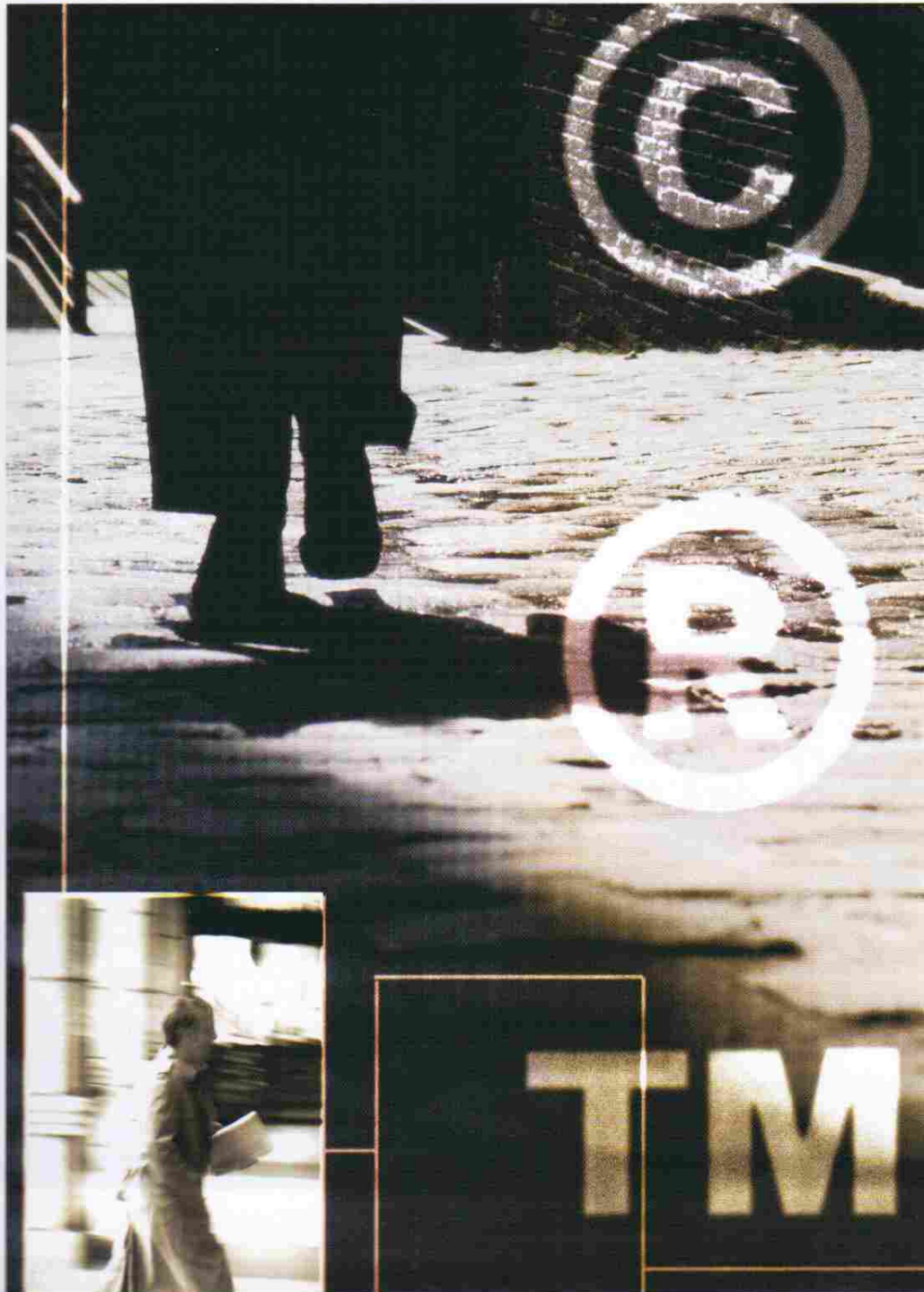
Regardless of its form, intellectual property is among a business's most valuable assets. It's this that helps them stay ahead of the competition – which is why protection is crucial. Unfortunately, IP in the form of precedents, templates, operational manuals, client lists, proposed marketing and business development plans, and other internal material are not generally registrable. As such, they are harder to protect from misuse.

"Once your IP is out the door, it's hard to get it back, because you've lost control of it and how it's used," says IP specialist Simon Singer, principal of David Landa Stewart Lawyers in Sydney. "It could be used in a manner that degrades the business name and reputation. As such, it can affect the goodwill in your business, or materially assist your competitors' business."

Singer says businesses need to adopt an IP-protection strategy that focuses on both internal systems and external elements – and be vigilant in their enforcement. A typical IP protection strategy includes carrying out an IP audit, education of staff, tight contracts with employees and third-party service providers, internal surveillance systems and active enforcement of IP rights.

IP AUDITS

An audit is a systematic review of all the IP used within the business. By documenting all its IP, including corporate knowledge and databases, the business can identify whether or not it owns all the IP, whether it's used effectively, and whether it's being threatened by competitors.



It's also a good idea to add IP to the business plan, give each a dollar value and include it in the balance sheet, and even implement them in the business strategy. It makes the business more attractive to lenders and the business community.

CONFIDENTIALITY AND STAFF EDUCATION

Confidentiality is the key issue – particularly if you're going to market with the IP. Identify any staff who are exposed to, or using, the IP. Educate them on the importance of confidentiality, and add a confidentiality clause to their employment contracts.

EMPLOYMENT CONTRACTS

"There are huge IP issues when you take the human element into account," Singer says. Contracts should state that anything created by the employee in the course of their employment is owned by the company, can only be used – with the company's consent – for purposes connected with the company's activities.

"Some contracts go even further, imposing a positive obligation on employees to notify the company as and when a breach (or suspected breach) of confidentiality arises. It is also important to ensure that when an employee leaves the company, he or she returns any business IP in their possession and remains bound by the confidentiality undertakings.

"Businesses should also ensure their staff manuals refer to IP ownership and confidentiality of information relating to the business and its customers/suppliers," Singer adds.

Contracts between a business and the consultancy to which it outsources are crucial, too. "Here, there are two things to think about: confidentiality and ownership of the IP," Singer says. Many smart business owners negotiate a clause into their service agreement that confirms all marketing material developed during the course of the client brief rests with the business owner, and must be returned when the service arrangement is terminated. "If possible, the service agreement should also state that the third-party service provider must obtain confidentiality undertakings from its own employees, to guard against the misuse of IP down the line."

SURVEILLANCE

Businesses are most vulnerable to staff stealing IP when they are about to depart. "The problem is that staff often make the decision to leave their job a few months before they tell their employer. Those two months are a very vulnerable time for the business, in terms of IP theft," says Singer.

Businesses need to implement strict internal systems of management and supervision in

order to ensure compliance with confidentiality requirements. Surveillance tools now available include sophisticated IT systems that allow businesses to track who downloads or opens documents; webcams in high-risk areas of the office; restrictions on the downloading, emailing and copying of large documents; various levels of security access into databases or accounting systems; security systems that allow the business to track which staff enter and leave the building and at what time.

USB ports can be locked off too, says Daniel Beer, managing director of Sydney-based IT services company Techknowledge Group. "And with Windows, there's a huge range of security settings to use, which will limit people from using it. But you can lock down a machine so much, you've made it virtually unusable and then you can lose productivity. It's a real issue for businesses concerned about IP. You need to weigh it up: what's the trade off between security and productivity? Because in today's businesses, you need to get the information out fast."

Beer says that when a staff member leaves,

businesses also need to identify what passwords and security codes they have access to, then change it and lock it down when they leave. "So many businesses don't think of that."

Businesses can also be vulnerable to ex-employees. "It's a good idea for business owners to keep an eye on their activities, too, to ensure confidentiality is being observed."

ENFORCEMENT

According to Singer, there is no point in negotiating a contract with an employee or third-party supplier if you are not prepared to take the extra step of implementing surveillance and enforcement procedures. "Unfortunately, legal proceedings are long and expensive and best avoided if possible. But at the end of the day if such systems are not enforced there is no use having them in the first place."

Beer says it is the small businesses that usually lack a sense of security. "Small businesses are the most relaxed about security and IP – many of them just don't think about it, but they need to." ■

