How can businesses protect their confidential information?

Q: I am in-house counsel for a global organisation and have been asked to advise on how we protect our confidential information. What factors should be considered when seeking to achieve this?

A: Every business has information it considers integral and invaluable to its success, and a competitive edge in the marketplace may rely on a business having or developing certain information above and beyond that of its competitors. In this challenging economic climate, the need has never been greater for employers to protect that information.

Confidential information can be subject to threats from outside the business owing to theft, hacking or commercial espionage. However, the biggest threat to confidential information often comes from inside the business. Many employees will have access to valuable knowledge about customer contacts and financial and strategic business intelligence in the course of their employment, all of which will be an attractive asset to any competitor seeking to encroach on the employer's market.

Employers can and should take steps at the beginning of the relationship with new employees to protect their trade secrets, confidential information and business contacts. Employers can minimise issues by:

- putting in place a tailored contract, including confidentiality provisions, restrictive covenants and a garden leave clause and keeping them under review as circumstances change over the life time of an employment relationship;
- limiting access to confidential information to those who require it and labelling documents as being 'confidential';
- including a confidentiality policy in the staff handbook that complements the confidentiality provisions in the contract of employment;
- putting in place a social media policy that sets out clear rules on the use of social media sites during working hours, on company-owned equipment and any equipment owned by employees. It should also contain rules about the disclosure on those sites of company information or information belonging to the company's customers and suppliers or other third parties. The policy should also state the extent to which (if at all) social media sites can be used by employees to store business contacts;
- implementing a strict electronic communications policy that clearly distinguishes between the rules for personal and business use.

The company's disciplinary policy should tie in and cross-refer to each of these other policies. The disciplinary policy should clearly state that misuse of confidential information will constitute gross misconduct and could lead to summary dismissal.

- carrying out training. Policies must be available and properly communicated to the workforce. They must also be complemented by appropriate and regular training. The training should reiterate the company's rules to ensure that employees are in no doubt about their obligations. Employers should ensure they take a register of attendees at training and that the attendance is recorded on the individuals' personnel files. This should assist the employer in demonstrating employee awareness of the information the employer deems to be confidential and employee knowledge of the rules regulating its use and disclosure should a dispute arise.

The number and type of disputes about misuse of confidential information and unlawful competition by employees and directors has significantly increased in recent years. The use of springboard injunctions together with damages claims provide employers with the ability to protect confidential information. Employees automatically have duties to their employers not to knowingly misuse or wrongfully disclose their employer's confidential information during employment. However, when employees leave their employment, the business can be less well protected.

Therefore, in drafting restrictive covenants, employers need to take into account:

- the role the employee will have in the business and the protection likely to be required should they leave to join a competitor. How are the business and the role likely to evolve?
- consistency of treatment across the business for employees carrying out the same type of role;
- not restricting the employee for any longer than necessary. If they are only going to have access to confidential information that has a limited shelf life before it is in the public domain, the duration of the covenants should reflect this;
- if the employing company is involved with different types of businesses, the employee should be restricted only in relation to the part of the business in which they were personally involved;
- avoiding drafting the covenants too widely. They should focus on prohibiting the activities in which the ex-employee was involved for the ex-employer; and
- if including a non-compete covenant in the contract, consider the appropriate territory for the restriction; the employee should not be prevented from working everywhere but only in the markets where the company does business and in which the employee was involved.

Protecting secrets

Changes within the workplace have also given rise to new challenges in protecting confidential information, particularly the growth of new technology and social media and the globalisation of business. With employees bringing their own electronic devices to work and social media allowing employees access to client contact information both inside and outside work, it makes protecting confidential information a constantly evolving area. Privacy and cross-border data protection laws add a further complexity. It is likely to be only a matter of time before such issues come before the courts. Litigation in the UK and elsewhere has also highlighted the difficulties associated with protecting confidential information cross-border.

Employers must therefore be urged to take a careful look at the information they are concerned to protect and to conduct an assessment of the risks that may result in its disclosure or loss. They should then consider the measures they have to take to achieve effective protection. In the current economic climate, employers cannot afford to be complacent; now is the time to equip the business with the tools it needs to protect its secrets and limit its exposure to legal risks.

Clare Gregory is a partner in the employment team at DLA Piper