How do employers protect data from theft by their own employees?

Stephanie Pritchett, Data Protection Lawyer and Consultant, outlines strategies that organisations can use to minimise the threat and/or impact of data theft by current and departing employees

A recent survey (by security company Imperva) established that 72% of employees in the UK have stolen data from their employer. In the majority of those cases, the employees stole the data using personal laptops, USB sticks and other portable storage devices including their mobile phones. In the same survey, 70% of the respondents indicated that they would consider taking information with them if they were to resign or to lose their job. Most surprisingly, 59% also believed that the information was theirs to take.

The statistics confirm that it is not just corporate spies or revenge-seeking employees that employers need to consider in protecting their data. It is every single employee, including those who, having found a new position, are wanting to get ahead, or those looking to sell the information for a profit or to set up in business competing with their ex-employer.

Another interesting survey was carried out by Orthus Ltd, a European information security risk management consulting firm, which analysed over 200,000 hours of user activity over a 2 year period. That survey identified that:

- 62% of data theft carried out was by people in IT or Customer Services Departments;
- 72% of the thefts occurred on Fridays between 3-5pm;
- 68% of the theft was linked to mobile devices;
- 48% used web mail, instant messaging or social networking sites to remove the information; and
- 36% copied information to a local drive or device.

Despite the above statistics, most instances of data theft can be avoided by employers having robust procedures and policies in place which employees are then educated about, and which are monitored and enforced in practical terms.

So what can employers do to protect themselves from such 'inside attack'?

Employers need to take proactive measures to protect their information from employees and departing employees. Some practical steps are considered in this article.

Increasing staff awareness

Employers should ensure that employees are made aware that the employer will most likely be the rightful owner of the intellectual property (IP) in the information. This means ensuring that employees are generally aware of the importance of data as a corporate asset, and also what the risks to them will be of using such information in unauthorised ways. This is important because, in the event of a dispute, the courts will look for evidence that the employer made it clear to employees that certain information was considered confidential.

Employers should also establish regular information security awareness training for all employees, and ensure that employees are trained generally in the company policies (including its data protection and data security policies). Employees should be well aware that confidential information and personal data cannot be used unless it is for legitimate business purposes and, where appropriate, for purposes justifiable under data protection law.

Confidentiality agreements

Under common law, a duty of good faith and fidelity and a duty of trust and confidence are implied into every employment contract. These implied terms require employees to act in their employer's best interests, and include respect for the confidentiality of the employer's commercial and business information, and a duty not to compete with the employer's business.

The scope and extent of the implied duty of confidentiality depends upon what type of information is involved. A body of case law has developed which differentiates between the

following different categories of information:

- Information that amounts to trade secrets or the equivalent – an employee must keep this kind of information confidential even after their contract of employment has terminated;

- 'Mere Confidential Information' - this is information which employees must treat as confidential during their employment, but which becomes part of the employee's general skill and knowledge base. This kind of information cannot be used by the employee to benefit their new employer while that employee still remains employed by the organisation. If, however, there are no express confidentiality restrictions in their employment contract which apply after termination of that contract, the employee will be entitled to use this information once their employment has terminated; and

- Information that amounts to the learned skill and knowledge of the employee or public information (such as information that the organisation has deliberately put into the public domain). These types of information are not proprietorial and cannot therefore be protected. This was held by the courts as far back as the 1916 case of *Herbert Morris Limited v Saxelby* where it was held: "To acquire the knowledge of the reasonable mode of general organisation and management of a business of this kind, and to make use of such knowledge, cannot be regarded as a breach of confidence in revealing anything acquired by reason of a person having been in any particular service, although the person may have learnt it in the course of being taught his trade."

Though it is beyond the scope of this article to consider these categories in detail, employers should note that it can sometimes be difficult to distinguish which information falls into which category. As always, organisations can benefit from a thorough analysis of all information held. Suffice to say, it is important for employers to ensure that relevant employees have express confidentiality obligations in their employment contracts to ensure that it (the employer) has the best chance of protecting confidential information post termination of employment. Employers must seek advice to ensure that the definition of 'confidential information' used in employment contracts is carefully and precisely drafted to ensure the best chance of the courts concurring that the information is capable of protection.

The recent case of *Brandeaux Advisers (UK) Ltd and others v Chadwick [2010]* highlighted the importance of the issue of confidentiality. In this case, it was held by the High Court that an employee was in fundamental repudiatory breach of her employment contract when she sent a large amount of her employer's confidential information to her personal email account. This breach entitled the employer to dismiss her without notice. The court remarked that the possibility of litigation with an employer was unlikely to justify an employee in transferring or copying confidential documents onto her private computer.

Post-termination restrictive covenants in employment contracts

Employers may also wish to ensure that express, post-termination restrictive covenants are written into appropriate employment contracts. These covenants can be written in a manner that aims to:

- prevent employees from working for competitor organisations for a defined period of time after leaving;

- prevent employees from soliciting previous customers of their ex-employer for a set period of time;

- prevent employees from poaching former colleagues; and

- restrict the use of confidential information relating to the ex-employer.

For these kind of covenants to be enforceable in the event of a dispute, great care needs to be taken in both the drafting of them, and in deciding whose contracts they should apply to. It will not be acceptable to have the same level of restrictive covenants put into all employment contracts. For example, it would probably not be acceptable for staff working in an in-house catering function at a law firm to be told they could not work for any other law firm for a period post termination. Employers will need to be able to provide evidence justifying the need for this kind of protection.

If an individual has not signed an employment contract with an express or adequate confidentiality obligation, employers may also seek to impose terms by way of a compromise agreement where one of these is being entered into.

Routine and random employee monitoring and auditing

Employers should exercise more caution around 'higher risk' employees, such as those who are being fired or made redundant and who may be likely to set up in competition with their previous employer or work for a competitor business. System administrators and technical or privileged users with more information access rights may also be in a higher risk category.

Employers should then be on the lookout for suspicious behaviour suggesting that an employee might be misusing confidential information or personal data. Such suspicious behaviour may include:

- Making extensive use of a personal email account (including through social media networks such as Facebook that may not be easy for the employer to track) ;

- Setting up LinkedIn or other corporate networking account and asking contacts to connect with them without their managers knowledge (particularly where those accounts are linked to their personal rather than work email address);

- Emailing documents to their personal email addresses or taking hard copy documents off site without permission;

(Continued on page 10)

- Asking colleagues or support staff to compile information (e.g. customer lists) without an obvious reason;
- Making contact with customers without their manager's knowledge;
- Using USB sticks or phones that connect to their employer's devices to download information;
- Making a large amount of photocopies for no particular reason; and
- Working unusually late or early hours.

This kind of employee conduct may be monitored via CCTV cameras, office entry and access systems, photocopier log in details, email monitoring, telephone logs and electronic document use tracking. Forensic IT investigators may even be needed to recover information when an employee thinks they have 'covered their tracks'.

While it may be appropriate to monitor the employee in this way, this will need to be done carefully to ensure:

- that the organisation does not breach the implied employment term of trust and confidence which could entitle the employee to resign and claim constructive dismissal, which could in turn invalidate the post termination covenants the organisation wishes to apply; and
- compliance with the Regulation of Investigatory Powers Act 1998, the Computer Misuse Act 1990 and the Data Protection Act 1998. In the case of the latter, this may mean that the employer has to have informed the employee about the monitoring taking place. Employers should therefore check that their own internal policies deal with this sufficiently, and that any monitoring takes place in line with the Information Commissioner's recommendations in Part 3 (Monitoring at Work) of the ICO Employment Practices Code (available for download on the ICO's website). If employees have been made aware for some time that, for example, their emails may be searched at any time, then it will be difficult for them to argue that the employer was doing this inappropriately.

Robust data protection and data security policies

Employers should also put in place and enforce stringent data protection and data security policies, procedures and technical measures to ensure that confidential information and personal data are protected.

In the case of personal data held by the company (customer lists and marketing databases, employee, donor, supporter or contractor information etc.), employers must remember that as a data protection legal requirement, they are required to take 'appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data'. What these measures should be will depend on the nature and size of the particular organisation, and the type of information that is being processed.

When considering data theft by employees and ex-employees, employers should make staff aware in their data protection and data security policies that:

- Particularly sensitive or confidential information should be protected by restricted electronic access controls, and employees should only distribute or share particularly sensitive information with limited privileged employees and users who have a need to know that information for their specific business purposes. It is harder to steal information if you have no access to it in the first place!;
- Particular categories and types of data will be considered to be confidential data or sensitive personal data and will warrant a higher degree of care when using and sharing that information. That information should then be clearly marked to make others aware that extra caution is needed. Appropriate steps to identify that information will depend on the nature of the data used within the particular organisation. It may, for example, be enough to identify what the confidential and sensitive personal data are within a policy. Perhaps clear "confidential information" markings should be added as watermarks or headers of documents, perhaps certain envelopes, emails or files should be marked "confidential", and perhaps certain information should not be shared electronically but only in a face-to-face scenario. Organisations need to carry out their own internal risk assessments into the types of information they hold and then make sure that employees are clear as to what is expected of them in the different circumstances;
- All mobile media use should be technically restricted and trackable;
- All organisational information must be returned to the employer before employees leave employment, and employees should be made aware that the information should be deleted from their personal USB sticks, laptops and phones;
- Confidential information and personal data should be password-protected or should be kept in locked cabinets. Where passwords are being used, they should be of adequate strength (less chance of them being cracked) and changed often. Employees must also be made aware that they are not authorised to share their account and log in details with other users;
- Employees' online actions will be logged, monitored and audited (where appropriate - see further below);
- Employees' computer access will be deactivated immediately following their termination of employment.

Organisations should also have social media policies in place to clearly define the expected use of networking websites such as LinkedIn (and if they do not already have one, now is perhaps the time to consider putting one in place). That policy can include statements to the effect that all contacts remain the property of the employer and impose obligations to delete

(Continued on page 11)

or return data from these sites to the company upon termination of employment. This is a relatively new area in the employment law arena so it remains to be seen how enforceable such policies will be. In the meantime, they should at the very least act as an effective deterrent.

Informal and formal steps to prevent use

Employees found to be in breach of their duties of confidentiality and data protection should be disciplined to demonstrate to them and all staff that the organisation treats these issues seriously, that policies will be enforced and disciplinary action will follow for anyone violating the rules.

In relation to departing employees, employers may wish to consider:

- Whether, in some circumstances, it is appropriate to ask the departing employee to agree to an undertaking that they will comply with their duties of confidentiality (a refusal may make the employer more likely to be on guard) or indeed to stop the offending behaviour if it has got that far. In either case, the employee knows their 'card is marked';

- Writing to employees before their employment ends, reminding them of the express and implied confidentiality and data protection obligations that apply to them during the remaining days of their employment as well as the post termination covenants that will apply;

- Whether it is reasonable to speak to their new employer informing them of the undertakings entered into or the post termination restrictions on the ex-employee. Essentially, such action serves to issue a warning shot that a claim against the new employer may be brought if they (the new employer) induce a breach of contract, or a claim for the tort of conspiracy may be brought if confidential information ends up being used by the new employer.

If all this fails and the employer feels that an employee has breached their confidentiality or data protection obligations or infringed database rights, the employer may need to start a legal action against the ex-employee, the new employer or certain individuals within the employment of the new employer requesting:

- An interim or springboard injunction if it can be proved on the balance of probabilities that the employee has been misusing or misappropriating confidential information or personal data or that they had the clear intention to do so; and/or

- Delivery up or destruction of confidential information and equipment (e.g. laptops, memory sticks, mobile phones etc.); and/or

- Some form of financial damages to compensate the organisation for its loss.

Conclusion - take extra care and be proactive

As part of general data protection policies and procedures, it is clear that organisations need to keep a close eye employees. The 'inside threat' is a serious one and could cause unparalleled loss to an organisation's personal data and confidential information.

It is essential to remember that loss of personal data, even to an employee or ex-employee, and unauthorised use could put an organisation in breach of its obligations under data protection law and may even be considered a reportable breach offence to the Information Commissioner's Office. The potential £500,000 monetary penalty from the Information Commissioner could make losing valuable company data even more financially damaging – all of which is avoidable with a little preventative policy work, training, monitoring and enforcement.

Stephanie Pritchett
Pritchetts
stephanie@pritchettslaw.com

Stephanie Pritchett leads the training course, 'Data Protection Essential Knowledge—Level 2' - for further details, visit www.pdptraining.com