
EMPLOYMENT

MAY 2008

THE THREAT FROM WITHIN: WHAT TO DO WHEN YOUR DATA WALKS OUT THE DOOR



Anthony Drake
SENIOR ASSOCIATE

Staff turnover is teaming up with technology to present businesses and organisations with a growing threat of cyber theft.

While stealing company property and information has been an age old problem, today's mobile workforce, assisted by computers and data-carrying devices, has introduced a whole new range of potential issues for employers to manage. While it's important to remember that most staff are generally honest, it does pay for organisations to consider how vulnerable they may be to cyber theft and to take steps to mitigate potential loss and business damage. Much like the exit interview, some employers may even wish to consider an exit audit.

When suspicion arises

While some employers are stung and end up with no, or after-the-fact, knowledge of theft, there are cases where behaviour may arouse suspicion.

Take this recent New Zealand case – not untypical of the type of theft that can occur.

Two days before resigning a senior manager remotely accessed the company's network from his company laptop and spent about five hours downloading what can be best described as sensitive and confidential

information - product lists, pricing lists, client lists and even strategic plans.

When he resigned he asked to take two weeks' outstanding leave before beginning his one month notice period. The company agreed and the employee took his two weeks' annual leave. He did not automatically return to work after this time as expected. The company asked him to return for a meeting but he refused. At the end of his notice period when he was handing in his company property, including the laptop, his manager asked him where he was going and what he was planning to do. The man was reticent – even reluctant – to discuss his future plans. His behaviour raised suspicion with the manager who was prompted to check the man's employment agreement. It contained a confidentiality provision, but no restraint of trade provision.

The company sought legal advice on reminding the employee of his obligations of confidentiality and a solicitor's letter was sent, bringing to his attention these obligations. The employee responded with his own solicitor's letter, saying that he was under no obligation and was not required to advise the company of his future plans. The response only heightened the employer's concern – it merely wanted to remind him of existing obligations.

Enter the forensics experts

The company decided it may be worthwhile investigating the employee's actions in the months before his resignation. It engaged a forensic computer expert. Very soon the computer examiner confirmed the company's worst nightmare. The departing employee had used the company's laptop to download such a significant amount of material (including confidential business information, strategy and financial information) that if it was printed out and stacked it would be half the height of the Auckland Sky Tower. The computer expert was also able to ascertain that the material had not only been downloaded to the laptop but had also been transferred to a USB key.

The company's solicitors again wrote to the employee's solicitors seeking the return of the material and the USB key. The employee's solicitors wrote back and advised that the employee had returned USB keys to the company and that he had not retained any information. The two USB keys were checked by the forensic examiner who confirmed that they were not used to transport the company's information. Obviously, a third key was used.

An application was made to the Employment Relations Authority claiming breaches of loyalty, fidelity, contract, good faith, and seeking an order for the return of the company's property, including the third USB key.

The Authority undertook an urgent investigation and issued orders including that the employee surrender the USB key to the company. When the third USB key was returned, the forensic examiner confirmed that the company information had been downloaded onto that device, but that it had later been deleted and the device defragged. (Defragging essentially wipes and rearranges files so they become incoherent and difficult to reconstruct).

Still, some material remained and the forensic examiner confirmed that the material had been downloaded onto yet another device.

Another application was made to the Authority seeking access to any other computer device the employee had, including his home computer. The Authority ordered the employee to surrender his home computer to the company for examination. The forensic examiner then found that just before it was handed over to the company, the home computer had been wiped and defragged.

The examiner also discovered the home computer had been connected to a printer and had been printing for five hours prior to the delivery. The forensic examiner was able to reconstruct parts of the wiped computer and confirmed that the employee had access to yet another device.

Access to that device – which was the employee's wife's laptop – was then sought. The wife's computer was found to contain some of the company's material, including emails.

Ultimately, the issue was resolved. A consent order was obtained from the Authority which included a restraint preventing the employee from using the company's information and working in competition with the company for a period of six months.

The company discovered that before resigning the man had accepted a job with a start-up enterprise that was going into business in direct competition to it. The start-up nature of the new business provided some explanation as to the level and volume of material the man had downloaded.

Key legal principles

Employees are subject to a number of common law duties to their employer, whether these are expressed in a written employment agreement or not. One of these is the obligation not to use or disclose confidential information. Employers can claim some protection of confidential information, even after the termination of employment and without any written agreement with the employee requiring confidentiality.

The more senior the employee and the more access they have to the company's confidential information, the more will be expected of them. When the use of confidential information relates to a trade secret, the implied duty of confidentiality will not disappear with the termination of employment.

The English Court of Appeal in the 1985 decision *Faccenda Chicken Ltd v Fowler* outlined factors which may be relevant to determining the degree of confidentiality of any particular piece of information, as follows:

- the nature of the employment – if the employee is habitually handling information that is sensitive, they could be expected to appreciate the confidential nature of it to a greater extent than if he or she only occasionally deals with confidential information;
- the nature of the information – the information must either be a trade secret or of such a highly confidential nature as to require the same protection as a trade secret;
- whether the employer emphasised the confidential nature of the information; and
- whether the information can easily be isolated from other information which the employee is free to use or disclose.

However, in its 1991 decision in *Lansing Linde Ltd v Kerr* the English Court of Appeal has shown a loosening of the Faccenda description of "trade secrets". It defines the meaning of "trade secret" as "information which, if disclosed to a competitor, would be liable to cause real (or significant) harm to the owner of the secret ... must be information used in a trade or a business, and ... the owner must limit the dissemination of it or at least not encourage or permit widespread publication".

This appears to be a preferable view of the meaning of trade secret in this context. It can include not only secret formulae for the manufacture of products but also, in an appropriate case, the names of customers and the goods which they buy. Some may argue that not all this type of information is a trade secret in ordinary parlance. If that view is adopted, the class of information which can justify a restriction is wider, and extends to some confidential information which would not ordinarily be called a trade secret."

It is the quality of the information, and the fact that its disclosure to a competitor would cause real harm to the employer, which is relevant in deciding whether the information is of a truly confidential nature, and not whether the information is of a technical nature or whether the employee has committed the information to memory.

Legal remedies

There are a range of potential remedies available to employers. An immediate one would be to seek a search and seizure order (Anton Piller) from the High Court.

There is also the ability to seek urgent directions from the Employment Relations Authority (exercising its powers under sections 160 and 173 of the Employment

To receive your updates faster, please subscribe to our electronic newsletter service on: info@bellgully.com

To view all our publications or update your details please visit our website: www.bellgully.com

For further information, please contact your usual Bell Gully adviser or:

AUCKLAND

Rob Towner
DDI 64 9 916 8902
rob.towner@bellgully.com

Christine Meechan
DDI 64 9 916 8927
christine.meechan@bellgully.com

Anthony Drake
DDI 64 9 916 8875
anthony.drake@bellgully.com

Naomi Cervin
DDI 64 9 916 8327
naomi.cervin@bellgully.com

Clare Abaffy
DDI 64 9 916 8896
clare.abaffy@bellgully.com

WELLINGTON

Andrew Scott-Howman
DDI 64 4 915 6820
andrew.scott-howman@bellgully.com

Maria Berryman
DDI 64 4 915 6546
maria.berryman@bellgully.com

Matt McGoldrick
DDI 64 4 915 6953
matt.mcgoldrick@bellgully.com

Disclaimer: This publication is necessarily brief and general in nature. You should seek professional advice before taking any further action in relation to the matters dealt with in this publication.

All rights reserved © Bell Gully 2008

Relations Act) regarding the preservation, use and return of the employer's property.

A complaint could be lodged with police. The Crimes Act was amended in 2003 to incorporate computer-based crimes provisions including:

- taking, obtaining or copying trade secrets (section 230);
- accessing computer systems for dishonest purposes (section 249); and
- damaging or interfering with computer systems (section 250).

These new provisions all provide for a term of imprisonment.

Key lessons

For employers there are some important points to note:

- Confidential information is important to most businesses, and protection of such information by employers can be of critical importance.
- A business can easily lose its competitive advantage if an employee takes confidential information to a competitor, solicits customers of the former employer or solicits other employees to resign and join the former employee.
- If an employee has access to the company's computer network, as part of the termination procedure an employer might wish to check whether the company's information, including confidential information, has been copied, downloaded or transported.
- Limitations should be placed on how much information an employee can download without first having to seek approval. For example, the ports on a laptop computer could be disabled as a preventative measure and if an employee needs to download a

document or material larger than a specified size, there could be an approval process.

Lastly, if there is any issue at all – don't delay. The longer an employer leaves the situation unaddressed, the more difficult it is to recover property and information.