The high cost of data thefts

By Fiona McLay, Special Counsel, Harris Freidman

- Data thefts are costly and they can affect small and large organisations with equal frequency.
- Forensic inspection can reveal incriminating behaviour such as copying and downloading files.
- Recent court cases show courts balancing the tension between allowing skilled employees to support themselves and protecting an organisation's work product.

Former employees taking company data to a competitor is an increasingly common problem. Three recent Australian court cases illustrate limits of court action and the importance of being proactive about protecting critical company data.

Media headlines capture attention and focus on serious privacy breaches like Australian Red Cross Blood Service who last year confirmed an embarrassingly large data security breach involving 1.2 million records.[1] But data theft from former employees is reported less often and it is difficult to measure how often it occurs. One global index records a malicious insider as the attributed source of five out of 44 data breaches in Australia in 2016 and seven out of 45 breaches in 2015.[2]

In a world where data is becoming an ever more precious commodity data thefts are costly. They affect small and large organisations with equal frequency. The costs to business, including those in Australia, have been extensively covered by the Ponemon Institute in the United States, which has conducted an annual study into data breaches and the cost to business since 2005. The institute's latest survey put the average consolidated total cost of a data breach at $4 million.[3] It reports that the biggest cost is lost business.

Company data: Lost in the cloud?

Enabling employees to work remotely increases the risk that valuable company information is stored on employee's mobile devices, which are often backed up to personal computers and cloud storage. It may be that departing employees are under the misapprehension that data they worked to create belongs to them. One survey by Symanec revealed that 62 per cent of employees think it is okay to store company data on their personal devices or cloud storage.[4]

Although an employee is entitled to use skill, experience and knowledge acquired in the service of a former employer in legitimate competition, an employer owns and can protect trade secrets and genuinely confidential information.

Whether particular information is confidential depends upon:

- if it is well known outside the employer's business
- the skill and effort used to collect the information
- has the information been treated as confidential by the employer
- the value of the information to competitors
- the ease or difficulty with which the information can be duplicated
- if common practice in the particular industry supports the claim for confidentiality.

Publicly available information is not confidential. For instance the phone number or email address of a person which appears on a website is not confidential. But where a company

has paid for the work done to collect a target list of people who need a particular product and the time frame when they are looking to buy, the target list could be confidential.

The growth of digital marketing using social media opens new areas of potential dispute over who owns information associated with a particular social media account. For example, there has not yet been a definitive decision in Australia on who 'owns' an employee's LinkedIn profile and connections. And this will depend on circumstances including how the LinkedIn account was set up, paid for and operated.

Prevention the best cure

The risk of data theft can be minimised by taking preventative measures such as:

- restricting access to confidential information for example using encryption or password protected files
- where software enables it, lockdown or restrict the ability to export data
- implement authentication of users
- regularly re-evaluate who has been trusted with access to company data
- set automatic notifications for suspicious database activity
- create and enforce policies for storage of client and prospective client contact information
- have a social media policy which specifies that the company owns information collected using the company's resources and require transfer of login details upon termination of employment
- where possible ensure social media accounts are created in a company name with company brand and using work contact details
- ensure no one person has developed, operates and controls critical software.

To protect your business from data theft it is essential to have effective post-employment contractual provisions that:

- identify the confidential information with accuracy
- impose restraints on a departing employee only as far as is necessary to protect the legitimate interests of the employer.

The same technology that enables the quick transfer of large amounts of data also leaves a digital record.

Use technology to prove data theft

The same technology that enables the quick transfer of large amounts of data also leaves a digital record. If you suspect data theft, it is important to act quickly to preserve digital evidence on any computer or device a departing employee has used. Even if files have been deleted and recycle bins emptied, digital footprints of the deleted files will remain. Forensic inspection can reveal incriminating behaviour such as copying and downloading files.

Where possible, devices (computers, mobile phones and tablets) should be turned off and set aside. If that is not possible, digital forensic tools enable an exact copy to be reproduced and preserved. Make sure Apple devices remain turned off until a copy is made so that they can't be erased remotely.

Getting back your data

Forensic evidence is usually sufficient to obtain search orders and orders for the return or destruction of stolen data. If the employee returns or undertakes to destroy the stolen data and to not use the information, unless there is evidence of actual misuse of the information, there will be a limit to what else you can achieve through court action. It can feel unsatisfactory to have to trust a thief to comply with an undertaking.

It's worth a look to see how recent court cases show courts balancing the tension between allowing skilled employees to support themselves and protecting an organisation's work product.

Account manager emailed contact list to himself

Last year, iseek Communications, an online cloud, data centre and connectivity provider launched proceedings in the NSW Supreme Court[5] involving a former employee, Mr Timothy Jones and his new employer Anticlockwise Pty Ltd. Mr Jones was account manager and sales engineer until he was made redundant by iseek.

Iseek consented to Mr Jones working for its competitor Anticlockwise provided he not work on sales that competed with iseek or contact iseek customers for six months.

Iseek then discovered that on the day his employment was terminated Mr Jones had emailed himself a contact list in a csv file. The list, compiled by Mr Jones, had contact details for iseek clients (as well as Mr Jones' friends and relations).

Iseek contended that Mr Jones breached his contract by using and disclosing information that was confidential to iseek from his contact list.

Mr Jones offered to undertake to not solicit iseek's customers, to delete permanently the file in question and to make an affidavit to that effect. Anticlockwise undertook that, until a final determination of the proceedings, it would maintain proper accounts and records to identify the terms of any contract, the identity of customers and the duration and consideration paid or received in relation to contracts entered into since Mr Jones began work with Anticlockwise.

The court took into account Mr Jones' personal circumstances and did not restrain Mr Jones' employment with Anticlockwise. Because iseek had sought an injunction despite the offered undertakings, iseek had to pay costs of the unsuccessful application to restrain Mr Jones working for Anticlockwise.

Sales representative copied entire customer list onto USB

A sales representative for SAI Global, Mr Liam Johnstone, began working

for SAI Global in August 2015, but resigned at the end of October, two months later.

SAI Global, previously known as Standards Australia International, runs integrated risk management assessments over tech platforms and also provides property settlement services. Three days before he resigned, Mr Johnstone copied two computer files containing confidential SAI information onto a USB Flash drive. And four days after he resigned, Mr Johnstone began work for a competitor of SAI and in the weeks that followed used the information on the USB flash drive to work out which customers of SAI were also customers of his new employer. He said he did this off his own bat without the knowledge of his new employer.[6]

One month later, SAI Global launched proceedings[7] and obtained orders for Mr Johnstone to hand over computers and storage devices associated with his employment. Within a week, Mr Johnstone complied producing a computer and USB flash drive, along with an affidavit admitting the material facts of the case. Mr Johnstone also admitted to breaching his employment contract with SAI Global and infringing their copyright on the computer files. He also admitted to breaching obligations under the Corporations Act, fiduciary duties owed to SAI Global and obligations in his employment contract concerned with working for a competitor of SAI Global during a period of two weeks following his resignation.

Mr Johnstone argued that SAI Global had recovered its information and it had not suffered actual damage. In the circumstances, he argued there was no grounds for a permanent injunction to restrain him using information he no longer had.

Although the judge was prepared to permanently restrain Mr Johnstone from using SAI Global's confidential information, he commented that once Mr Johnstone had delivered up the stolen files it had not been necessary for SAI Global to continue the proceedings. SAI Global was only entitled to 50 per cent of its costs since Mr Johnstone complied with the order to deliver up material.

Mr Johnstone had to repay $4,230 (two weeks salary paid to Mr Johnstone after his resignation), nominal damages $1 for copyright infringement and $5,000 additional damages for copyright infringement because of the flagrancy of the infringement.

Graphic designer allegedly copied entire database

While the Ponemon Institute's 2015 Data Breach study[8] lists higher data breach costs for industries in health, pharmaceutical, financial, energy and transportation, data breaches can also be proportionally damaging to industries in fashion and retail.

Online fashion retailer, Showpo, for example, alleged in the Federal Court that a former employee and graphic designer, Ms Melissa Aroutunian took a database of 306,000 contacts including customers and suppliers and supplied that information to Black Swallow, which Showpo claimed presented itself as an affiliate of Showpo.

The dispute settled in April, this year, with Black Swallow ordered to pay ShowPo $60,000 in compensation and Ms Aroutunian permanently restrained from using or disclosing the contact list but each side paid their own legal costs.[9]

While responding to questions from a journalist at the Australian Financial Review[10], the managing director of Black Swallow, Mr Alexander Baro, said that the allegations were 'garbage' and denied his company was in possession of a customer list or that he had paid Ms Aroutunian for a client list saying, 'Nah, we bought her a house'. His statements, which may reflect on the cavalier attitude many in business have toward data theft, also included telling the AFR to 'write whatever you want ... use your imagination, I can't wait to see what you come up with.' ◪

Fiona McLay can be contacted on (02) 9023 9114 or by email at fmclay@hflawyers.com.au.

Notes

1 www.afr.com/technology/web/security/red-cross-apologises-after-mass-leak-of-australian-blood-donor-records-20161028-gscyfc

2. Gemalto Data breach index http://breachlevelindex.com/data-breach-database

3 https://securityintelligence.com/media/2016-cost-data-breach-study/

4 www.theaustralian.com.au/business/technology/data-theft-linked-to-ex-employees/news-story/824778be2f85a1e49497bef8d93c7166

5 Iseek Communications Pty Ltd v Jones [2017] NSWSC 251 www.austlii.edu.au/au/cases/nsw/NSWSC/2017/251.html

6 www.austlii.edu.au/cgi-bin/sinodisp/au/cases/nsw/NSWSC/2017/251.html?stem=0&synonyms=0&query=Iseek%20AND%20Jones

7 www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/FCA/2016/1333.html?stem=0&synonyms=0&query=title(SAI%20Global%20and%20Johnstone%20)

8 www.jmco.com/media/Ponemon-Data-Beach-2015-Report.pdf

9 www.afr.com/technology/web/security/black-swallow-settles-showpo-data-theft-allegations-for-60000-20170411-gvidya

10 www.smh.com.au/business/retail/showpo-sues-fellow-eretailer-over-data-theft-20170116-gts7eu.html