benchtv
a benchmark production

Précis Paper

The High Cost of Data Theft

There is a need to act quickly if there is a suspicion that information has been taken and there needs to be an appropriate response if such a situation arises. Resolution often occurs when there is an undertaking by the former not to use the information. The best protection from data theft is to keep control of your information by locking it down and having correct contractual protections in place in an employee's employment contract.

Discussion Includes

- Why is there an increase in data theft?
- How do people take information out of an organisation?
- The information required for a forensic expert to determine whether some material has been taken
- The appropriate response to the information that has been taken
- The requirement that the information is confidential
- The need to act quickly
- New Mandatory Notification of Data Breach Laws
- Contractual preservation
- Other mitigating steps

Précis Paper

The High Cost of Data Theft

1. In this edition of BenchTV, Fiona McLay (Special Counsel at Harris Friedman, Sydney) and Rod McKemmish (Principal at CYTER, Sydney) discuss the importance of acting quickly when data theft by a former employee is suspected, mitigating factors to prevent it occurring, and the need to keep costs in perspective.
2. There are three critical steps when data theft is suspected:
   (a) Act quickly as soon as you become suspicious and how to get forensic evidence about the theft;
   (b) Objectively assess what has been taken and what you can do recover it; and
   (c) Make sure that you have the right contractual protection and proper data hygiene to limit the harm that can be done.

<u>Why is there an increase in data theft?</u>

- Organisations are becoming more aware of the issue
- Greater awareness of the value of the information
- The ease with which the information can be taken has increased
- Employees take information when they go to set up a business in competition
- Customer information, whether it is a list of customers or a complex customer database, can be the lifeblood of a business and business owners often perceive its loss as devastating because of the potential flow on effect on the business cash flow..

<u>How do people take information out of an organisation?</u>

- Email - logging onto a web-based connection and emailing themselves information
- Draft emails with attachments means there is no transmission of the email
- USB Storage Devices eg thumb drive or hard drive
- Cloud-based storage eg Dropbox Box, OneDrive
- Remote Access Tools eg TeamViewer
- Social media
- Cloud backups
- Hot spotting or tethering - bypassing the firewalls
- Bring your own device (BYOD) – internal storage and as a conduit to cloud storage

<u>The information required for a forensic expert to determine whether some material has been taken</u>

- The dates and times of employment and suspicious activity
- Passwords and user account details
- What systems did the employee have access to as part of their employment eg Dropbox

- Does the organisation install data privacy tools which wipe it
- Does the organisation install specific tools to administer the laptop remotely eg: TeamViewer
- The History of the computer eg replacing the hard drive
- Do not turn on their laptop – it will destroy the evidence trail!

3. Conducting a "forensic triage" on the laptop which differs from a full forensic analysis in that it looks for the forensic indicators that suggest the use of USB storage devices, cloud storage, web based emails etc… The key to doing a triage is:
    - Preserving the original laptop.
    - Taking a forensic copy of the key artefacts.
    - Don't turn the laptop on or use it.
    - If indicators are found then a decision can be made as to whether a full forensic analysis is required. At this time it is best to talk to a lawyer to determine the value in proceeding.
4. In *SAI Global Property Division Pty Ltd v Johnstone* [2016] FCA 1333, the business development manager had taken a list of clients. After establishing that the file had been downloaded onto a USB drive, the company went to Court and sought some orders for delivery of that file, the computer and the computer that the employee was using at their new job. They continued to seek a permanent injunction to restrain that employee from using that information and continued with their forensic investigation of other documents that he may have used. The company was successful in proving that there had been a breach of its copyright and a breach of the contract of employment. However, the Court was not prepared to let them recover the full amount of the damages that they had incurred because the information was recovered so quickly.
5. After the delivery up of the stolen list and his computer, further forensic examination of his computer revealed that a second file containing customer opportunities had been copied and that (while he was working for SAI Global) Mr Johnstone had emailed himself information which was confidential to his former employer before SAI Global. So SAI Global were presumably concerned about whether he could be trusted. Mr Johnstone gave evidence that of his own bat (not involving his new employer) he had used the client list to compare it to the new employer's client list. He hadn't otherwise used the information and hadn't contacted any of SAI Global's customers. Mr Johnstone objected to a permanent injunction restraining him from using SAI Global's information on the basis that he had returned the information immediately once caught and had co-operated, there was no evidence that SAI Global had suffered any loss of sales.
6. The Judge did grant a permanent injunction. It also awarded nominal $1 for breach of copyright, $5,000 damages because of flagrant infringement of copyright and damages for breach of the employment contract equal to two weeks salary paid to Mr Johnstone in advance (during which he had worked for his new employer). When it came to costs, the Judge found that SAI Global's costs of the proceeding of about $275,000 were

disproportionate to the importance and the complexity of the issues in dispute. The Judge found that SAI Global had the most important relief that it sought within a week when the list was delivered up. Mr Johnston had admitted breach of copyright and breach of employment agreement in the defence. Although SAI Global had been successful, it could only recover its costs up to the delivery up order and of the second forensic examination of the computer that was delivered up. This case shows that organisations can get emotionally invested in revenge and matters of principle but you need to keep an eye of what is proportionate

7. From a forensic perspective, when an employee takes company information a digital trail will:
    - Be dependent on the method used and the type of device used.
    - Typically would look like this:

<u>USB devices</u>

- Details (make, model and serial number) about devices connected to a computer
- Dates and times of various connections

<u>File activity</u>

- Evidence of mass copying
- Details of files accessed on external storage devices
- Details of folders accessed on external storage devices
- Dates and times of when the computer / device was used
- Geolocation of device.
- User accounts used to access devices or files.

<u>Access to cloud based storage</u>:

- Copies of files synchronised to a cloud storage account (e.g. drobox)
- Evidence of deletion of files from a cloud based storage account.
- Sharing of files with other users via a cloud based storage account.

<u>Email activity</u>

- Via corporate system
- Web based email

<u>Connection activity associated with:</u>

- Network devices
- WIFI hot spotting / tethering

<u>The appropriate response to the information that has been taken</u>

8. There are a number of cases where injunctions have been refused due to the requirement to establish that the information that has been taken is confidential information that the company is entitled to protect.
9. In *Iseek Communications Pty Ltd v Jones* [2017] NSWSC 251, Mr Jones had emailed to personal email account a list of all of his Outlook contacts, which includes customers but also his friends and family. The judge found that the circumstances in which the contact list

was forwarded didn't suggest that he was intending to misuse the information. He accepted that the undertakings offered by Mr Jones and his new employer were sufficient and would not grant an injunction restraining him from working.

10. In *Sprout Network Pty Ltd v Roth* [2017] NSWSC 1717, the employee had emailed about 30 clients, copying his personal email address, advising that he was leaving and inviting them to keep in contact with him through LinkedIn. The employer sought an injunction that Mr Roth deliver up any list of customers, price lists or confidential information. The judge refused to make an interlocutory injunction. There was no evidence that Mr Roth had taken customer lists or price lists. There was no contractual restraint preventing him from competing. He was entitled to use information that he had acquired in the course of his employment. The email addresses of clients were publicly available, being published on various websites. It was not a taking of confidential information

<u>The requirement that the information is confidential</u>

11. It could be an embarrassing result to rush up to Court to seek an injunction for information that does not have the appropriate nature of confidentiality. Factors that the courts will use to determine if the information is confidential include:
    - How that sort of information is treated in the industry and how closely protected it is;
    - The time and effort that goes into compiling that information;
    - How it was treated by the employer;
    - How it was communicated to the employer - whether it was described as confidential;
    - The value of the information how easy it would be to replicate; and
    - Whether that information is commonly known in the industry.
12. In *Capercorp Pty Limited v Brasam Pty Limited as trustee for Brasam Investment Trust* [2017] NSWSC 608, the franchise's menu was held not to be confidential - it was available on their website.

<u>The need to act quickly</u>

13. In *Optiver Australia Pty Ltd v Tibra Trading Pty Ltd* [2007] FCA 2065, Optiver was an arbitrage business which had developed software that enabled it to detect discrepancies in share prices. A number of former employees established a business in competition. Optiver was suspicious that Tibra had copied the source code for the software. It was suspicious because it knew how long it had taken to develop its software and Tibra had got similar software very quickly.
14. Another example where this might occur is an in-house employee for a software development company who moves to a competitor or a contractor who will have a library of code that the use for different projects. Today source code is very much when people develop solutions they're integrating third party technologies or code into it so they might have to open source code that they put in. There is no confidentiality around it because you can get it from a repository like GitHub. The complexity in a source code comparison

is identifying what is third party, what is reuse and what is unique. You need to do enough investigation to be able to make sure that there has been some unlawful taking. However, if you wait too long you can get into a situation where there's been so much independent effort put on to whatever software may have been taken that it's very hard to prove what the damage is and to quantify that loss.

15. Optiver made an application for preliminary discovery of the source code which Tibra was using about a year after Tibra had started. The judge refused the application for preliminary discovery. One of the reasons for refusing it was because Optiver had failed to satisfactorily explain the delay in starting the case. He accepted that Tibra had been working on its software for a year and had significantly changed the software over that time. The comparison with what was alleged to have been stolen would not be useful.
16. Having open source or third party version control of your software is good practice.

New Mandatory Notification of Data Breach Laws

17. The Mandatory Notification Scheme commenced in Australia on 22 February 2017. It is regulated by *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth). Businesses who have a turnover of more than $3 000 000 are governed by those Australian Privacy Principles.
18. Once you suspect there may have been an eligible data breach, you have 30 days to assess whether there has been a breach and whether you need to notify affected persons and the Office of the Australian Information Commissioner.
19. 30 days is a very tight time frame. Some of these systems are very complex and sometimes the data is not always necessarily sitting in Australia and you may need to rely on a third party to provide you with information.
20. A big problem are third parties holding data for a company who are supposed to maintain their security so will not disclose information to protect their own liability

Contractual preservation

21. Contractual rights in employment contacts that define the information that a business owns can be used to mitigate data theft. They can be utilised to ensure that the information remains the business' property throughout their employment and after termination of the employment.
22. In *BlueScope Steel Limited v Somanchi* [2016] FCA 4, urgent ex parte orders were made for a former employee suspected of taking 40 gigabytes of data including proprietary software to deliver computers and passwords to an independent expert.
23. There could be a contractual mechanism in an employment contract where the employee has to disclose what information they have or not.
24. One case, which settled according to newspaper reports, involved a graphic designer who allegedly copied a database of 306,000 customers and suppliers and gave it to a competitor. According to newspaper reports the competitor paid compensation and the

graphic designer was permanently restrained from using the information. A good question – does your graphic designer need to be able to download your entire customer database?

25. Show that a process of taking steps to protect the information and limit people who had access to it can be used to establish that the information was confidential and valued by the company

Other mitigating steps

26. Locking information down and controlling access by keeping it stored in one central place rather than try to patch it up later to mitigate or limit the amount of damage.
27. When an employee flags that they're leaving:
    - Understand why they're leaving;
    - Where they are going to;
    - What information did they have access to;
    - If they were to take that information what value is it for a competitor
28. The courts attempt to balance allowing someone who's developed skills and knowledge to use that skill and knowledge to support themselves and protecting a company's work product. The courts are also mindful that a company had an ability to control the contractual protection of the information during the employment relationship.

BIOGRAPHY

Fiona McLay

Special Counsel at Harris Friedman, Sydney

Fiona is an experienced litigator who acts for individuals and small to medium sized companies in a wide range of commercial litigation matters with a focus on resolving disputes between business co-owners and shareholders. Prior to joining Harris Freidman in October 2007, Fiona worked for two national law firms where she focused on insurance litigation including coverage advice and defending negligence claims against hospitals, doctors, engineers, universities and other professionals on the instructions of their professional indemnity insurers. She regularly posts on Linkedin, Twitter @BreakupBusiness and Instagram @BreakupBusinessLawyer.

Rod McKemmish

Principal at CYTER, Sydney

Rod is the Principal at CYTER. Rod has over 20 years of experience providing Forensic Technology and Cyber Forensic services to organisations and their legal teams. Rod's work experience includes preparing expert reports and performing forensic examinations for matters involving employee misbehaviour, theft of confidential information, data breaches, intellectual property disputes and general technology disputes. Rod has provided expert reports for matters in Australia, New Zealand and Hong Kong.

BIBLIOGRAPHY

Cases

SAI Global Property Division Pty Ltd v Johnstone [2016] FCA 1333

Iseek Communications Pty Ltd v Jones [2017] NSWSC 251

Sprout Network Pty Ltd v Roth [2017] NSWSC 1717

Capercorp Pty Limited v Brasam Pty Limited as trustee for Brasam Investment Trust [2017] NSWSC 608

Optiver Australia Pty Ltd v Tibra Trading Pty Ltd [2007] FCA 2065

BlueScope Steel Limited v Somanchi [2016] FCA 4

Legislation

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)