Forensic IT Postcard

Ferrier Hodgson

August 2015

WHEN YOUR IP LEAVES WITH YOUR STAFF

As technology continues to evolve and new methods to store or transmit electronic data come into fashion, what assurances do you have that your intellectual property hasn't walked out the door with your former employee who has joined a competitor or launched a new business?

This scenario is a common problem. Unfortunately by the time you realise that Newco is using your customer list and intellectual property, your data has already left the building. Our experience investigating these matters often finds suspicious copying of commercially sensitive material in the days or weeks leading up to the employee's final day. There have even been cases where the employee had been harvesting precedents, templates and client data nearly a year prior to their resignation.

Detection readiness

Locking down a business environment so severely in an attempt to thwart IP theft can effectively cripple many of the business' processes. Modern organisations rely upon flexibility and the quick movement of electronic data to operate effectively. Company directors and business owners may struggle to achieve the right balance between data freedom and data security so that employees have sufficiently flexible access to commercially sensitive material whilst maintaining organisational control over that data.

Permanent prevention is almost impossible to achieve, and largely comes down to the continual formulation, implementation and communication of appropriate policies, which must be regularly updated for technological evolution. For example, organisations need a clearly communicated policy regarding the use of cloud based storage services.

Permanent prevention is almost impossible to achieve, and largely comes down to the continual formulation, implementation and communication of appropriate policies, which must be regularly updated for technological evolution.

Detection, on the other hand, often requires the creation and preservation of a sufficient electronic evidence trail. Increasingly, organisations have policies to forensically preserve computer systems, mobile phones and network storage for critical employees in their exit process. Preserving and retaining these forensic copies is not expensive, and acts as an insurance policy in the event of future problems. Once a forensic copy is taken, computers and phones can be decommissioned or repurposed without destroying potential electronic evidence. The continued use of a computer after the departure of an employee, especially by your own IT department, risks contaminating vital evidence.

"It looks like they've got all of my templates – and my client list!"

While consideration should be given to what copies an ex-employee may legitimately take, for example personal files and public information, it is obvious a copy of “client list.xls” with the folder “Precedents & Templates” is a serious concern. Identifying proof of the theft, including when and how, generally requires an expert forensic examination. Evidence must be thorough and clear to support any applications for injunctive or other forms of relief. In many cases, the quality of the evidence uncovered has warranted the need to seek an ex parte procedure such as an Anton Piller order.

To provide rapid and cost effective forensic analysis, our experience provides us with the knowledge of where to look for relevant evidence. Historically this has been employees sending information to web based email addresses or taking copies on USB devices or CD/DVD. While such methods remain common and form part of our initial analysis, we are seeing more and more employees utilising a myriad of cloud based storage services including Dropbox, Google Drive and Share File.

In a recent engagement, we established a user activity timeline that linked:

- The user of interest accessing various client and marketing lists within a short period of time.
- The insertion of a USB device.
- Folders being created or accessed on that USB device.
- One of the key client list documents being later accessed from the USB device, proving that it had actually been moved onto the device.

We were also able to identify the serial number of the USB device in question so that delivery-up demand for access to that specific storage device could be made.

In other engagements, we have correlated access to key documents and network locations with access to cloud storage services such as Dropbox, and also the generation of a disproportionate number of hardcopy print jobs run by an outgoing user during their final days of employment.

“They’ve got my IP – how do I get it back?”

“Regaining control” of electronic data has been debated extensively in the media. When looking at the latest celebrity photo leak or hack it is clear that once the electronic cat is out of the bag, it is very difficult to get the original cat – plus any copies of that cat – back in the bag.

One remedy we have assisted with is to forensically examine the ex-employee’s computers, USB devices and other media, and then securely delete files which impinge on a company’s IP in a manner preventing them from being recovered. This action is usually arranged by court order or agreement and, while it is not a complete guarantee that other copies do not exist, when combined with a written undertaking from the infringing party that no further copies, backups or works based on those documents exist does provide some level of relief to the aggrieved party.

Once the electronic cat is out of the bag, it is very difficult to get the original cat – plus any copies of that cat – back in the bag.

Michael Khoury
Partner
Sydney
+61 2 9286 9864

Sean Powell
Director
Perth
+61 8 9214 1409

Forensic contacts

Justin Geri
Senior Manager
Melbourne
+61 3 9604 5142

Scott Arnold
Director
Brisbane
+61 7 3834 9213

Jean-Pierre du Plessis
Partner
Adelaide
+61 8 8100 7696

Ferrier Hodgson’s Forensic IT specialist Michael Khoury regularly sends a *Forensic IT Postcard* detailing the latest news and trends in the sector. If you have any comments or suggestions, please contact Michael directly at michael.khoury@fh.com.au. If you know of others you think would be interested to receive the *Forensic IT Postcard*, please send us their details.

If you would like to change your subscription details click here and select "Want to know More?".

If you wish to see previous editions of the Forensic IT Postcard click here.

Ferrier Hodgson

For more information about our services, please contact one of our offices. Or find out more at: **www.ferrierhodgson.com**:

Sydney: Steve Sherman
+61 2 9286 9905
steven.sherman@fh.com.au

Adelaide: Martin Lewis
+61 8 8100 7657
martin.lewis@fh.com.au

Perth: Martin Jones
+61 8 9214 1405
martin.jones@fh.com.au

Malaysia: Andrew Heng
+60 3 2273 6227
aheng@fhmh.com.my

Melbourne: Peter McCluskey
+61 3 9604 5109
peter.mccluskey@fh.com.au

Brisbane: Will Colwell
+61 7 3834 9205
will.colwell@fh.com.au

Singapore: Tim Reid
+65 6416 1400
tim.reid@fh.com.sg