
Intellectual Property Theft — Unearthing the Electronic Evidence

Mark Garnett and Tabitha Bauer MCGRATHNICOL

Intellectual Property (IP) results from the application of someone's mind or intellect to create something new or original. IP can exist in various forms; it can be an invention, a brand name, a book, film, trade secret, the product of commercial activity or artistic design. Much of an organisation's IP is stored electronically and is generally accessible to a number of people. Due to the nature of electronic data, combined with the advent of smaller and smaller electronic storage devices, it is becoming easier to transport valuable IP, intentionally or otherwise, outside an organisation, thus making it vulnerable to loss or theft.

Even if an organisation implements internal security measures to protect their data, there is still a risk that a departing employee, or executive, takes IP with them that they are not entitled to. The gravity of the risk increases when the former employee is moving to a competitor organisation and the information taken is commercially sensitive.

Common escape routes

There are two common ways for IP to be removed from an organisation — sending the data out of the organisation via email or removing the data by physical means, such as copying it to a USB memory stick. Organisations are commonly under the mistaken belief that if the corporate email system is monitored then it is impossible to send data out via this method, which is simply not the case. Most people have — or are at least aware of — webmail services such as Hotmail and Gmail. An employee would merely need to access their webmail account via the Internet and use it to mail data out of the organisation and the corporate email system would be none-the-wiser.

The growing popularity of USB memory sticks also represents an enormous risk for organisations, with most having no security measures that prevent their use. These devices can be as small as a fingernail and are quite capable of storing hundreds of thousands, if not millions, of documents and they present a real risk if not controlled. Even more creative instances exist where IP

can, and has been, removed using digital cameras and iPODs. These can act just like a USB memory stick and can store any type of document, such as spreadsheets and reports.

Growing, in terms of risk and frequency, is the threat from external sources as evidenced by the recent hacking of Sony's PlayStation network. On this particular occasion, over 100 million users' account information was accessed by hackers and it would be naive to think that this type of attack could not happen to any organisation in today's business environment. The consequences to an organisation's reputation resulting from such an attack can only be imagined but suffice to say, awareness and prevention can go a long way to reducing the nature of this risk.

An ounce of prevention...

Organisations are recognising that IP is a valuable asset and are taking steps to prevent its theft in the first place. Mitigation requires both the education of employees and the implementation of technical barriers.

The education of employees regarding the risks associated with IP cannot be underestimated and as always, prevention is much better than cure. Technology barriers are also something that can be implemented without requiring inordinate investments in time or money. Restricting the use of webmail in organisations is a common preventative measure as is preventing the use of USB memory sticks or at least restricting their use to organisationally approved devices only. This provides some control over the transmission and copying of organisationally sensitive IP.

It is also encouraged that organisations implement a policy where devices and data that are used by key staff are captured upon their departure regardless of whether there is a suspicion of IP theft or not.

Additionally, document management and control systems play their part in monitoring who is accessing what documents on a corporate network. While of itself, a document management system will not prevent the theft of IP, it can certainly help the investigation of such incidents by creating and retaining audit logs showing who has accessed and copied documents and when this activity occurred.

Inhouse Counsel

The best laid plans...

Whilst prevent prevention is an important weapon in an organisation's defence against IP theft, it must be prepared for the worst, should these preventative mechanisms fail. Unfortunately, no level of prevention is one hundred percent effective and there may come a time when an investigation is necessary.

If an organisation suspects that it has suffered the theft of valuable IP, the typical recourse is to seek legal advice as to how they may be able to retrieve their IP and/or obtain compensation for its loss. In this instance, it is advantageous to seek the assistance of a suitable qualified technology advisor to collect, identify, interpret and present any electronic indicators of IP theft in a report or affidavit as early as possible.

Fight technology with technology

Many indicators of IP theft are stored in volatile areas of a computer system and are subject to modification or deletion through continued use of the computer. It is therefore critical that if an organisation intends to legally pursue a theft of IP, electronic devices used by the employee, such as a laptop computers, are identified, quarantined in a secure location and are not used until analysed.

It is wise to make this identification and isolation of data a priority in order to maintain the integrity of the data. It is a simple process to quarantine and preserve electronic information, but it is near impossible to recover from a situation where this has not been performed. Importantly, one need not have knowledge of computer systems to successfully take this important first step. The most common sources of indicators of IP theft include, but are not limited to:

- Desktop, laptop or tablet devices;
- Mobile phones;
- External storage devices such as USB thumb drives;
- Corporate email accounts including employee assigned mailboxes or shared mailboxes that an employee may have had access to;
- Internet history logs;
- Document repositories on the organisation's network that contained the valuable IP; or
- Document repositories on the organisation's network that were assigned for exclusive use by the employee. This location is often referred to as a "Home Drive" or a "Personal Drive".
- The quarantine of computer devices such as those listed above ensures that any indicators are preserved and allows for the best opportunity to perform a comprehensive and effective analysis.

- Another advantage to isolating these devices is that it gives an organisation time to plan a suitable response to the situation. The beauty of electronic data is that it can be left in quarantine for as long as required until an analysis is needed.
- It is obviously not feasible for an organisation to quarantine a server however these sources of information should not be ignored. The quicker relevant information from these types of data sources is extracted the greater the chance that the information will be useful.

Making sense of the 1's and 0's

Indicators of IP theft can include something as overt as an email sent to a recipient who is clearly not entitled to the information contained within the email. With employees becoming more aware of their use of technology often these indicators will be more subtle. Uncovering this information requires a more in-depth analysis to locate and, perhaps more importantly, interpret and present in a format suitable for use in legal proceedings, such as an affidavit or expert report. The next question is — What can a Forensic analysis of the data reveal?

The most common first step in a forensic analysis is to review the employee's computer or laptop and create a timeline of the employee's electronic activity over the period before their departure. This information can identify a change in user behaviour during this period in comparison with earlier activity. This may also include the commencement or the increase in frequency of copying documents to an external device such as a USB thumb drive. It may also include accessing an organisation's document repositories that contain sensitive documents that were previously not accessed by the employee or is not congruous with the employee's role. Once a timeline is constructed, unusual activities can be used as a starting point for more in-depth analysis of the computer and other devices.

If it is determined an employee used an external USB thumb drive to copy sensitive documents, analysis can be performed to identify and extract information on when the USB device was first connected to the computer, what documents were copied to the USB drive or when these documents were copied. This information can be retrieved from the employee's computer even if the USB device is no longer available for analysis.

Most USB thumb drives have a unique serial number that is assigned by the manufacturer and can be used to uniquely identify the device. The serial number, make and model is recorded by a computer's operating system. This information is useful if it becomes necessary to request the device from the employee for the purpose of retrieving the lost IP or to perform further analysis.

Sensitive documents are easily transmitted to external email accounts that are beyond the control of an organisation. The use of webmail accounts leaves traces on the computer from where it was accessed. The Internet history can show a pattern of access to a webmail account, such as Gmail or Hotmail, such as the frequency of access during the period before the employee's departure.

While there is recourse for obtaining private emails from accounts that are managed by local Internet Service Providers, such as Telstra Bigpond or Optus Home, service providers such as Hotmail, Yahoo or Gmail are almost impossible to retrieve information from without the consent of the user or through legal means. In these cases, often the user is compelled by Court Order to provide the login details so that the email from their account can be downloaded into an appropriate format for review. The risk is that there can be an opportunity for the user to login prior and remove any emails of interest and, once deleted, these emails cannot be recovered.

Mobile phones are a rich source of emails, SMS messages, documents and calendar appointments that may be pertinent. If the mobile phone is also synchronised with a computer then synchronised backups can be a good source of information, and if there are multiple backups available over a period of time, it may then further serve as a source of historical information. Technology today allows for the capture of data from mobile devices, including iPhones, with relative ease

and also, in some cases, allows for the recovery and analysis of previously deleted data, such as deleted text messages.

Documents themselves can be an important source of information. Many document formats, such as Microsoft Office documents, maintain internal properties known as metadata that describe the document including the creation date, modification date, last accessed date, last print date, name of the person that created the document, list of the last 10 authors to modify the document, etc. Some of these properties can be viewed and modified by the user but others are hidden and can only be retrieved using specialised tools. This data can be crucial in identifying who last opened and edited a document or, in some cases, copied the document.

IP can be an organisation's most valuable asset but protecting it can be a challenge. If the matter requires further investigation for the purpose of recovering the IP or seeking compensation for its loss, a forensic practitioner can assist in analysing the relevant computer systems and document the findings for inclusion in any proceedings. There are no guarantees that you will find a smoking gun — but your chances of success are greatly improved if the computer hasn't been touched in the interim.

Mark Garnett
Partner
and
Tabitha Bauer
McGrathNicol