

## Intellectual Property – Managing the Threat from Within

Intellectual Property (IP) can be an organisation's most valuable asset and yet is often the least protected. Companies will spend large amounts of time and money to install security measures to ensure their data is protected from external intruders, yet ignore internal threats. There is no doubt that protection from external threats is a necessity - yet relatively little thought is generally given to protection from those within the organisation. With most of an organisation's IP stored electronically, the biggest challenge is trying to control which employees have access to it and, most importantly, what they can do with it.

With employees increasingly working remotely, IP can be copied and stored in so many different locations that it is nearly impossible to monitor it all. Risk of IP loss can come in two different guises:

- + Accidental loss by employees whilst working with IP from remote locations, such as home or on public transport; and
- + Deliberate theft by employees who have access to the information and wish to use it for personal gain.

The challenge for an organisation is how they can monitor or control it without impacting on productivity.

### Two common escape routes

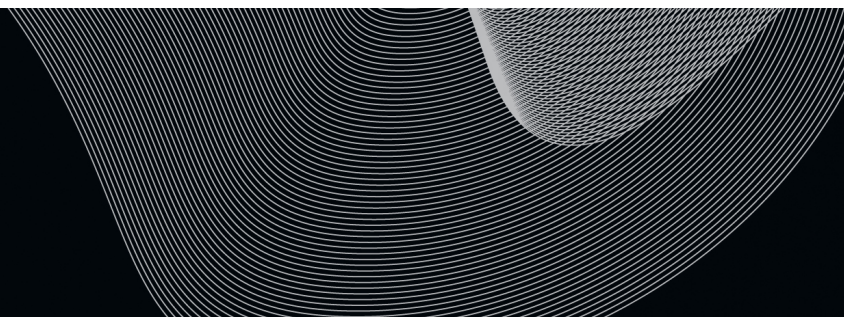
There are two common ways for an employee to remove IP from an organisation - send the data out of the organisation via email or remove the data by physical means, such as copying it to a USB memory stick. Organisations are commonly under the mistaken belief that if the corporate email system is monitored then it is impossible to send data out, which is simply not the case. Most people have - or are at least aware of - webmail services such as Hotmail and Gmail. The 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 of documents. They present a real risk if not controlled. We have even seen more creative instances where employees have removed IP using digital cameras and iPods. These act just like a USB memory stick and can store any type of document, such as spreadsheets and reports.

### An ounce of prevention...

All is not lost, though - organisations can take steps to prevent IP theft in the first place and to also mitigate the consequences should it occur. 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.



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

### **In case of emergency...**

So if an organisation suspects that this has happened to their IP, what recourse do they have? One of the first steps should be seeking legal advice on how they may be able to retrieve their IP and obtain compensation for its loss.

Indications of IP theft can be located on a computer used by an employee or on the organisation's network. This will often require the assistance of a forensic practitioner to identify, interpret and present these indications in a report or affidavit.

Many of the 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 investigate a possible theft of IP, any laptops or computers used by the employee are quarantined in a secure location and are not used until analysed.

### **Can you find the smoking gun?**

A forensic analysis can reveal if an employee has accessed webmail or has used a USB memory stick thus providing evidence that can either confirm or rebuff any suspicion that they have taken something that they should not have. More specifically, a forensic analysis can reveal the following:

- + If a user has formatted a hard drive or memory stick in an attempt to hide their tracks. Contrary to popular belief, formatting does not erase the contents of a disk drive;
- + Whether or not the user has accessed files stored on a corporate network just prior to leaving;
- + Determining if an employee has connected any removable storage, such as USB memory sticks, to a computer system and copied files to that device;
- + What Internet sites an employee has visited, which is recorded by default by all popular web browsers in use today;
- + The names of any files that may have been copied from a corporate computer system onto a privately owned storage device; and
- + What webmail the employee may have sent or received prior to leaving the organisation. Most computer users are under the mistaken believe that webmail offers an anonymous and undetectable way of moving information into and out of an organisation.

The Microsoft Windows operating system records a myriad of information "behind the scenes" unknown to the computer user that can be used to determine all of these facts and more.

IP can be an organisation's most valuable asset but protecting it can be a challenge. By being aware of the risks and taking steps to manage them, such as those discussed in this article, it is possible to minimise an organisation's exposure. Further, having effective policies in place will make it easier for an organisation to identify how the loss occurred. Finally, 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!