This article was published in the August 2017 issue of the
Singapore Law Gazette, the official publication of the Law Society of Singapore.

# Protecting High Value Intellectual Property in the Competitive "Innovation" World

**Gino Bello**
Senior Director, Technology
FTI Consulting, Singapore
E-mail: Gino.Bello@fticonsulting.com

Singapore is known for being a financial hub, is one of the world's most business-friendly markets, and renowned for its infrastructure. Well supported by its government, Singapore is also an "innovation nation", a proving ground for the latest and greatest technologies. Startups are naturally thriving here, given that Singapore itself is a 70-year-old startup success story.

## Competition in the Innovation Nation

But it's competitive. With a softening labour market and the unemployment rate rising, the value of developed technologies and intellectual property ("IP") increases. Employees and external parties recognise this. A recent article estimates that theft of trade secrets and software by South East Asian countries costs $600 billion a year.[1] Another recent study reported that almost two out of three departing employees take confidential or sensitive business information with them.[2] Done without the employer's permission, the confidential data can be easily accessed and remains portable beyond the employer's control.

## The Costs

Beyond the monetary and reputational loss to business, workplace theft of data – whether considered proprietary, confidential, copyrighted, or otherwise damaging in the hands of a competitor – remains problematic. Often times, the theft occurs at the hands of departing employees, either hoping to get ahead at a competitor, form a competing enterprise, or profit from the sale of the data.

In a conundrum to organisations – accessibility versus security – stealing data in today's digital world is fairly easy. Many organisations' most valuable assets take the form of digital information, from customer contact databases, sales and marketing information, business and strategy plans, designs and formulae, research, to lines of source code. Downloading, saving and transmitting this data can take as little as a few seconds and mouse clicks.

## Protecting High Value IP

Fortunately, this same digital technology that allows for ease of theft also arms investigators with a stockpile of techniques to compile a case against data thieves. Computer forensics specialists are the detectives of the 21st century. Through expert analysis, they can interpret subtle clues left by thieves to create a comprehensive account of the theft and identify the compromised data. With the evidence compiled by digital forensics experts – evidence that should be gathered in a highly defensible manner in case of future legal action – organisations can mitigate the potential damage and bring the bad actors to justice.

## Profiling and Preserving

Once an organisation suspects it has become the victim of data theft, a suspicion often aroused when a key employee defects to a competitor, employers and their legal counsel should consider taking swift steps to bring in computer forensics specialists to preserve the former employee's IT assets. This may require the legal department serving as liaison between the corporate IT department and the outside forensics specialists to determine the spectrum of IT assets that the employee may have had in his or her possession.

IT should suspend any data destruction or retention policies that could inadvertently destroy evidence. Once the departed employee's assets have been determined, the forensics team can create forensic images of hard drives, as well as secure copies of e-mail, network folders, use of document management systems, and customer relationship databases. With regards to forensic images of laptops, desktops, or mobile or portable devices, forensic

analysis is performed on exact copies to preserve the original data for law enforcement or trial.

## Types of Digital Evidence

More common assets include organisation laptops, desktops, e-mail accounts, smartphones, external storage devices, and network storage areas. Newer, non-traditional types of digital evidence can include social media and open source intelligence, GPS data, language and sentiment analysis via communication avenues, other activity-based mapping paths, and "clickstream" analysis.

Sometimes, an organisation may wish to conduct its own initial investigation. However, such actions may lead to unintended consequences. For example, opening a file on a desktop may alter the file's metadata and call into question its authenticity and future admissibility, which would be equivalent to trampling over a culprit's footprints at a crime scene.

## Rebuilding the Timeline – Analyzing the Evidence

Once the data forensics experts have taken the preliminary steps to preserve the employee's IT assets, analysis can begin. Whether for large or small-scale IP theft, collusion of employees to set up a competitor, or inappropriate access by privy employees, skilled forensics investigators have a number of methods they use to piece together the actions of suspected data thieves. These digital clues help to build a timeline and compose a picture of both what the employee may have done, as well as the employee's actual intent, whether it was nefarious, or simply accidental or negligent.

Within the Microsoft Windows operating system, the Windows Registry database stores user options, configuration settings, and also maintains an activity log that tracks when a user inserts an external storage device, such as a flash drive, into the computer's USB port, for example. This can prove to be a critical piece of evidence, as theft via flash drives and other portable external storage devices is one of the most common methods of data transfer. Sometimes, simply by looking at the date the flash drive was inserted and comparing it to the date the employee departed the organization, forensics experts can begin to build a case. Similarly, evidence of cloud storage usage such as Dropbox and OneDrive can be uncovered, adding to the timeline.

File metadata can provide clues into the actions and intent of a departing employee. Windows uses this metadata to report what files were most recently opened. A skilled data forensics expert can contextualize this data along with other findings to help pinpoint potentially compromised files, as well as the intent. For instance, after an individual copies files to an external device, he or she may open those files to ensure they copied successfully. By determining when an external device was connected to the computer and the level of sensitivity of the files last opened, data forensics specialists can begin to tell the story of the employee's final actions prior to leaving the organisation.

## Threats from the Cloud

The corporate world has begun to embrace cloud-computing applications that allow employees to access solutions wholly in an online hosted environment, which adds another layer of considerations for preventing and investigating IP theft. Applications such as a customer relationship management ("CRM") or a document management system ("DMS") software contain valuable, sensitive information that can range from client lists, marketing strategy documents, minutes, to billing models. The ease in which this data can be accessed, whether within the organisation or remotely from an employee's home, as well as the importance of the information, makes these cloud applications highly appealing to would-be data thieves.

A data forensics expert can analyze the departed employee's Web browser artifacts to determine when these cloud-based applications were accessed. This tactic, combined with data gleaned from the operating system registry and file metadata, can help determine whether this information was copied to a text-based file on the desktop or transferred to an external device. Further analysis of a CRM or DMS can also assist in building the timeline and intent of a departing employee. Have they been accessing or downloading more information than they typically have? This type of activity can be detected proactively (not just reactively) so that potential "flight risks" can be identified.

## Proactive Measures

Experienced computer forensics specialists can use their combination of technological and analytical skills to preserve digital evidence and tell the story of the data, not just in protecting IP, but also when digital evidence is crucial to building a case.

To better protect your organisation and implement strong safeguards, organisations can take the following proactive measures:

1. Categorise – know the location of all data and its value. If an issue arises, knowing exactly where the relevant data is stored, enables the team to focus an investigation on specific data sources, whether servers, cloud providers, applications, computers, or other devices.
2. Conduct regular cyber risk and information governance reviews to mitigate the risk of data theft. Where appropriate, seek independent, external advice.
3. Proactivity and awareness – iterative training to employees on the consequences of misconduct should be considered. Forensically image employees' devices whom are privy to high value information, regardless of whether there any allegations. It is cost and time efficient and retains key digital evidence if issues arise in the future.
4. Think outside the box – what applications (e.g. CRM, DMS, chat logs, SPAM filter) can be leveraged to detect behavioral changes that suggests impending departure of employees?
5. Consider overt or covert investigations. There are advantages to both. In addition to training, an overt investigation may assist in understanding the mindset of would-be data thieves.

In the age of information workers, easy access to organisation data provides numerous benefits, such as greater employee collaboration, productivity and mobility. Yet it can also heighten the risk of data theft. It is essential for organisations and legal counsel to act swiftly to protect the organisation's information-based assets, both reactively and proactively.

Gino Bello is a Senior Director in the Technology segment at FTI Consulting and is based in Singapore. A computer forensic expert and certified Computer Examiner, Gino specialises in forensic collection, analysis and expert reporting of digital evidence. He has led a broad range of matters including large-scale, cross-border disputes, arbitrations and e-Discovery engagements in class actions and royal commissions. He also assists clients in Cyber risk and incident response. Gino has led investigations into IP theft, information leakage, anti-bribery and corruption, regulatory and other employee-related misconduct.

**Notes**

[1] <http://www.business-standard.com/article/pti-stories/china-is-the-world-s-principal-ip-infringer-us-watchdog-117022700607_1.html>

[2] <https://www.gvsu.edu/e-hr/how-to-avoid-employee-data-theft-62.htm>