The Five Biggest Fallacies About Theft of Intellectual Property

"If a man keeps an idea to himself, and that idea is taken by stealth or trickery, I say it is stealing. But once a man has revealed his idea to others, it is no longer his alone. It belongs to the world."

- *Anonymous*

I want to start with a story of how China stole an entire aeroplane… In October 2018, ZDNet ran a story on how China's efforts into establishing a foothold in the aviation industry by building its home-grown plane left a trail of hacks across the aviation industry.

Through a coordinated approach, "contractors" (such as hackers, cybercriminals) are hired and assigned the theft of particular interest. If they cannot gather intelligence, Chinese intelligence will recruit company insiders, or even coercing Chinese employees to aide their hacking efforts using blackmail or threats against families living at home.

According to the security firm Crowdstrike, the end goal was to acquire the needed intellectual property to manufacture all of the C919's components inside China.

An accusation filed in California on October 25, 2018, charged 10 Chinese individuals with conspiring to steal aerospace trade secrets from 13 western companies, most of the U.S. based. The indictment also revealed that French aerospace manufacturer Safran was infiltrated when employees in its Suzhou,

China office inserted malware into the Safran computer network. This malware gave Chinese agents access to Safran's confidential files.

According to U.S. Trade Representative Robert Lighthizer, China's IP theft costs the US between $225 billion and $600 billion each year.

What is Intellectual Property?

Intellectual property is the production of new ideas you create and own by your organisation that is critical in achieving its missions.

The type of intellectual property are varied:

- Proprietary software / source code
- Business plans, proposal, strategic plans
- Customer information
- Product information (designs, formulas, schematics)

Some example:

- KFC – It's their recipe
- Coke Cola – It's their recipe
- Tesla – It's their software
- Google – It's their search engine

What is insider theft of intellectual property?

It is defined when an insider steals proprietary information from the organisation.

Some known examples:

- In January 2019, Apple accused one of its employee for stealing over two thousand files containing confidential and proprietary Apple material, including manuals, schematics, photographs and diagrams relating to its company's self-driving car.
- In July 2019, Tesla accuses a former engineer of theft of files containing Autopilot source code to his personal iCloud account in late 2018 while still working for the company.

- In January 2020, a former SoftBank Corp. employee was arrested for allegedly passing proprietary information from the major phone carrier to officials at Russia's trade representative office in Tokyo.
- In March 2020, a former Google employee was charged with stealing trade secrets from its self-driving car program.

What is the impact of insider theft of IP?

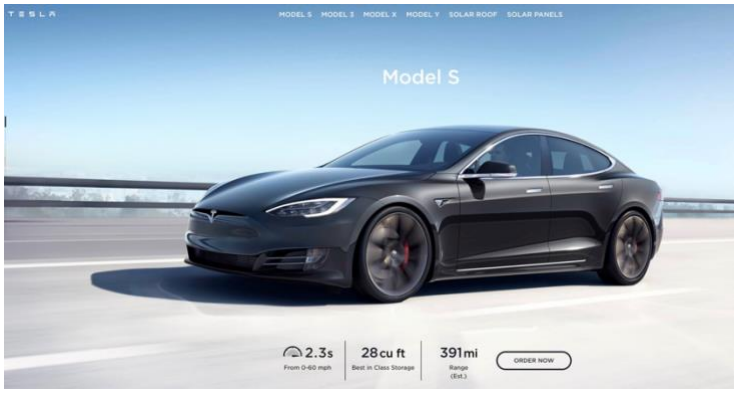
The impacts of insider theft of IP can be devastating. Trade secrets worth billions of dollars have been lost to foreign countries, competing products have been brought to market by former employees and contractors, and invaluable proprietary and confidential information have been given to competitors.

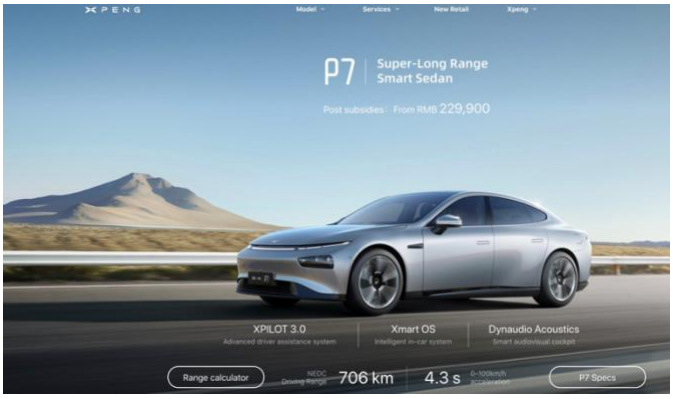
The following list the five fallacies that business thinks about Intellectual Property Theft.

IP Theft Fallacy #1

Very few insiders ever steal intellectual property to sell it. Instead, they steal it for a business advantage either to take with them to a new job, to start their own competing business, or take it to a foreign government or organisation.

Here is an example: A Chinese EV startup Xpeng, have stolen some of Tesla intellectual property, but it's not stopping the company from straight-up copying its website design too.





IP Theft Fallacy #2

There is a misconception that the IT administrators are the biggest threat.

Many people believe that because they hold the "keys to the kingdom", that they would be the prime suspect for theft of IP. According to Insider Threat Division of CERT, there is no observable case in their database which shows IT administrators stole intellectual property.

Those that steal intellectual property are usually current employees who already have authorised access to that IP (around 75% according to the insider Threat division of CERT). Such as engineers, programmers, or salespeople.

IP Theft Fallacy #3

There is a misconception that organisation high-level security technologies such as SIEMS will be able to identify and prevenet IP theft.

Technology is not able to recognise human behaviour from logs and system events. You cannot infer logs to reveal peoples intention and motivation.

Did you know, that "**dissatisfaction**" played a significant role in many of the IP thefts? Dissatisfaction notably resulted from the denial of an insider request, which in turn decreases the person's desire to contribute and diminish loyalty.

Yet, machines are not able to recognise "negative emotions" as a risk and businesses regularly miss these "red flag" behaviour warnings.

Importantly, you cannot detect theft of IP until the information is in the act of being stolen. In other words, the window of opportunity can be quite small.

That's why it is essential to pay close attention when you see potential physical behaviour indicators of heightened risk.

IP Theft Fallacy #4

The misconception that IP theft took place after hours and required sophisticated hacking.

Not so! Most of the IP was stolen during business hours and within one month of resignation using a variety of methods.

Most of these crimes tend to be quick thefts around resignation. But some of them stole slowly over time, committing their final theft right before departure.

"All of us have the right to change jobs, but none of us has the right to fill our pockets on the way out the door. "

- *US Attorney David L. Anderson*

IP Theft Fallacy #5

There is a misconception that IP theft is only conducted by a single person.

IP theft can be initiated by a person that may not have access to the IP. Insiders can be recruited or coerced into providing the IP.

According to the Insider Threat Division of CERT, around 33% of IP theft were the benefit of a foreign government or organisation.

What Can You Do to Mitigate Theft of Intellectual Property?

To prevent your intellectual property from walking out the door, consider the following set of recommendations.

Review employee contract

- Employees do bring information with them and possibly competitive and stolen IP from their previous employer. Be aware that your organisation may be liable for the theft. As part of your IP agreement that you make

new employees sign, include a statement attesting to the fact that they have not brought in any IP from any previous employer.

- It is inevitable that many of your employees will move to other businesses at some point in time. As soon as a person turns their resignation, you need to be prepared to act. Identify what information they are accessing. Identify movement of that information 30 days prior to resignation and 30 days post-resignation.
- Establish consistent exit procedures which should include – Access termination procedures; Ask departing employees to sign a new IP agreement reminding them of the contents of the IP agreement while they are walking out of the door; Review your termination policies and processes.

Periodically review and adjust your access controls.

- Many insiders at the time of stealing information, had access above and beyond what their job description required.

Monitor user anomaly activity.

- Monitor online and social media actions. These sites allow employees to easily share information about themselves as well as organisation details. Establish a social media policy that defines the acceptable use of social media and information that should not be discussed or shared online.
- Monitoring of data movement such as unusual activities - large attachments; printing sizeable documents; copying or downloading certain information.
- Tracking of all documents copied to removable media.
- Preventing or detecting emails to competitors.
- Targeted monitoring of users when they give notice of resignation.

Pay attention to physical behaviour

- Dissatisfaction, disgruntlement, or a negative argument over their entitlement may lead them down the path of IP theft.

How Can We Help you?

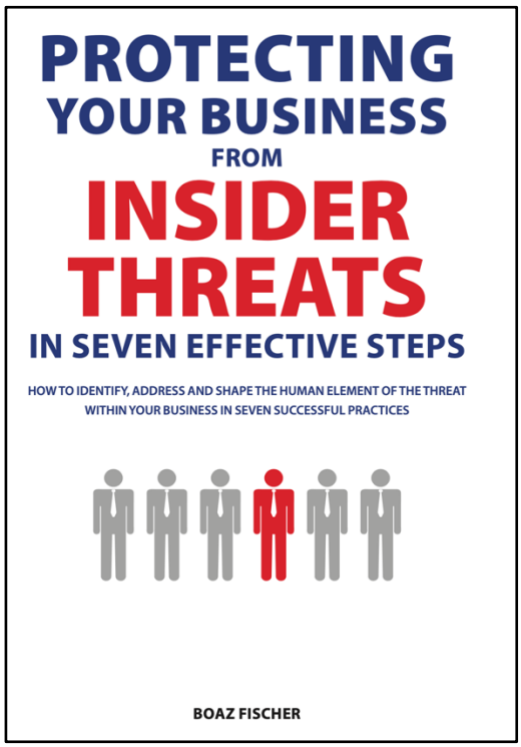
Are you concerned about the insider risk to your business?

Do you have critical intellectual property that you need protecting?

Have you been impacted by insider theft?

Do you need to comply with regulations showing that you have the right insider risk protection methods in place?

If so, reach out to CommsNet Group - https://commsnet.com.au/contact-us



Free Insider Threat Book

"How To Protect Your Business from Insider Threat in 7 effective Steps" by Boaz Fischer

- You can download your FREE copy **HERE**