INSIDER RISK
HIGH-TECH INDUSTRY

+31 70 22 11 940 Signpost Six www.signpostsix.com

HIGHLIGHTS

In 2023, a former executive of a leading chipmaking powerhouse was indicted on suspicion of stealing company technology to be implemented in a copycat factory sponsored by a foreign nation-state. The estimated value of the intellectual property theft amounted to $230 million. Whilst the attempt to build the plant failed due to funding issues, the theft posed a serious threat to the country's national economic security during a period of intensifying competition in chip manufacturing.

ABOUT US

As the leading insider risk management firm, we secure employees and organisations via a holistic approach towards insider risk management, vested in the best practices from across the globe. With our team of experts, we implement tailored solutions addressing every organisation's unique security challenges.

KEY FACTS

- As of 2020, the FBI had been investigating over 1,000 cases of Chinese theft of U.S. technologies.
- 55% of integrated circuit manufacturers report encountering counterfeit versions of their technologies.
- The average cost of data breaches in the technology sector, including those committed by insiders, amounts to $4.66 million.

WHAT IS INSIDER RISK?

Insider risk refers to the potential for employees, contractors, or other trusted individuals within an organisation to intentionally or unintentionally cause harm, such as data theft, sabotage, or fraud. This risk stems from their authorised access to sensitive information, systems, or assets. Effective insider risk management combines proactive measures and employee training to safeguard the organisation's resources and reputation.

Koninginnegracht 62, The Hague, NL

The development of these technologies is highly knowledge- and capital-intensive. The tech race between geostrategic rivals has seen the deployment of aggressive tactics to access Western technologies to aid economic and military development.

Insiders, thanks to their privileged access to sensitive information, are those best positioned to obtain, steal and compromise high-value data.

Today's Challenges

- It has been established by the Dutch General Intelligence Security Services (AIVD), that **foreign intelligence** agencies are aiming to build a network of sources to acquire knowledge and technology within leading organisations in the high-tech sector. The case affecting ASML in early 2022 saw an employee bringing intellectual property to Chinese-backed Huawei. Amid increasing geopolitical tensions, ASML and other European and American semiconductor companies have accused China of stealing not only intellectual property but also talent.
- The high-tech industry is the industry with the **highest rates of employee turnover**, standing at 13.2%. This stands as an emerging risk related to departing employee data theft, with 12% of departing employees admitting to taking proprietary information with them to their new employer.
- **Procurement and foreign investment** also increase the vulnerability of proprietary technology. Highly sensitive information is shared throughout procurement or public tendering processes. These can showcase expertise whilst also providing external with privileged access to key information and technology. European countries like Denmark have seen large debates unfold on whom to assign the development of 5G networks, accounting for the development of strategic high-tech dependencies.

Backdoor competition

- High-tech innovations such as AI, quantum computing, and chip manufacturing have become strategic assets for nationals and organisations seeking to gain competitive advantages. The potential dual use of high-tech innovations see the blurring of lines between economic and military power. The theft of proprietary knowledge plays a key role in advancing national capabilities, whilst damaging the efforts of organisations investing in the development of proprietary technologies through unfair competition.

- Currently, the U.S., Japan and the Netherlands provide around 90% of all equipment used in computer chip factories globally. These nations are enforcing strict export controls, making insiders who transfer their expertise and knowledge to foreign rivals crucial facilitators.

- Third-party collaborations, especially with academic institutions, represent an additional vulnerability to the high-tech sector. The strong ties between knowledge institutions and the high-tech industries are crucial to maximise development. Knowledge institutions, however, are strategically targeted by foreign actors aiming to build networks of professionals. University researchers may conceal their obligations to other knowledge institutions or talent programmes, getting privileged access to partner data.

- The necessity of keeping innovative prospects secrets enables insiders to possess non-public information potentially deployable for insider trading. Insider trading erodes market confidence, inhibits capital investment and directly harms investors.

Act Now: Insider Acts are growing in occurrence in the high-tech industry, costing businesses revenue and reputation. Protect your organisation from internal threats with our robust insider risk management solutions at Signpost Six. Don't delay, contact us today to fortify your defences and safeguard your trustworthiness.

+31 70 22 11 940 info@signpostsix.com

Visit our website for more!