INSIDER RISK
DEFENCE SECTOR

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

HIGHLIGHTS

Shapour Moinian, an employee of an aerospace defence contractor sold sensitive information regarding aircraft design for the U.S. military in exchange for $22,000. In 2021, an Italian Navy captain working at the office of the Chief of Defence was arrested for selling sensitive military documents, including NATO documents. Everette Hale committed an unauthorised disclosure to news outlets, containing classified information on U.S. drone attack capabilities, opera and details on target identification methods.

ABOUT US

As a leading insider risk firm, we secure employees & 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

- Top-100 arms-producing companies totalled a combined $592 billion in sales.
- More than 40 raw materials are deemed critical for strategic European defense.
- 32% of leading defence contractors are vulnerable to ransomware, with compromised credentials and poor internal practices.
- Of the top-100 defence contractors, 72% experience a credential leak every 90 days.

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

Sign post Six

WHERE PSYCHOLOGY MEETS TECHNOLOGY

Espionage, data theft and unauthorised disclosures account for the most significant share of insider acts in the defence sector.

- **Espionage refers to targeting domestic organisations or government entities to benefit a foreign state knowingly. Economic espionage aims to acquire trade secrets and intellectual property to drive innovation, strengthen a manufacturing position or modernise militaries.**
- **Data theft entails the insider's use of access to steal or exploit data, material and intellectual property, or IP, from an organisation.**
- **Unauthorised disclosures are the communication or physical transfer of classified information to an unauthorised recipient.**

Today's Security Challenges

- The **geopolitical environment** is the greatest driver of market growth, but also competition and espionage. As geopolitical tensions rise, so do the clandestine activities. Specifically, crucial contractors directly supplying large armies are under threat. However, many SMEs are also increasingly vulnerable to nation-state espionage as they do not have the financial, personal, and technical resources to train employees and create adequate technical and physical countermeasures to preserve information and assets.
- **Supply chains** are under pressure due to a shortage of certain components subject to trade restrictions and shortages. The vast amount of suppliers and raw materials the defence sector relies on increases their susceptibility to supply chain disruptions. These are crucial components of aerospace and defence systems which rely on these for performance and future innovation. In the U.S., a staggering 87% of defence contractors do not meet supplier performance risk system requirements.
- **Digital espionage capabilities** are now being combined with traditional espionage efforts. This has made economic espionage by nation-states the greatest threat to innovative advancements within the defence sector.

Defence From Within

- The high sales and expenditure levels show the increasing importance of defence manufacturers due to the current geopolitical context. Interstate military competition is becoming a national security priority of large military powers, making cost-effective R&D procurement an increasing priority.
- Clandestine agencies are increasingly able to detect individuals under pressure from financial, professional and personal stressors, creating the conditions to leverage an insider to commit espionage. For example, 78% of workers who left their positions within the sector were seeking better pay due to financial difficulties.
- The high levels of unauthorised disclosures and leaks are calling for better whistleblowing and reporting mechanisms for employees, and for enhanced data monitoring and vetting procedures.
- The emerging reliance of the public sector on the private sector is a recent development presenting emerging and distinct risks. For example, private third-party contractor partnerships also represent a great risk due to their access to sensitive data regarding military operations, capacities, and innovation, which can then be shared with clandestine services or competitors, as outlined by the Shapour Moinian case.
- Ideological motivations are increasingly relevant for intentional insiders in an industry defined by military objectives and national security, as outlined by the Rowe Jr case.
- The skill shortage faced by the defence sector creates an increased threat of insider risk. Worker attrition ranges between 10-15%, and the hiring objectives of various defence contractors are not being met. As a consequence, some workers have to work overtime and relocate, potentially creating environments where professional stressors are more common.

Act Now: Insider Acts are growing in occurrence in the defence sector, costing businesses costs in revenue and reparations. 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!