





INSIDER RISK ENERGY SECTOR

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

HIGHLIGHTS

In 2014, a Belgian Doel Nuclear power plant employee caused damages of over €300 million through sabotage. In 2021, an employee who used a VPN password in an unsecured network led the "Colonial" oil pipeline to suffer a ransomware attack by a hacker group, costing \$4.5 million in ransom and triggering a state of emergency in the U.S. Coercion and corruption are also increasing in the energy sector as the December 2015 attacks on the Ukrainian power grid show.

KEY FACTS

-  The average cost of insider acts in the energy sector is of \$14.45 million
-  The energy sector is one of the three sectors which falls victim to espionage the most
-  Human elements, such as error or malice are found in 74% of cybersecurity incidents in the energy sector.
-  Hornet Security lists the energy sector as the greatest target for cyber attacks in 2019, attracting 16% of all incidents

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.

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.



Sabotage & Espionage account for the greatest share of insider acts in the energy sector.

- Sabotage is a deliberate act aimed at undermining or incapacitating an organisation through obstruction, disruption, or destruction.
- Espionage refers to targeting domestic organisations or government entities to knowingly benefit a foreign state. The objective of economic espionage is acquiring trade secrets and intellectual property to drive innovation, strengthen a manufacturing position or modernise militaries.

Today's Security Challenges

- The interconnected nature of the energy sector with almost every other industry, and society more broadly, makes the energy sector a key player in economic, geopolitical and environmental issues.
- Digitalisation is providing innovation but also straining grid networks, broadening the attack vectors drastically, and creating a significant increase in the amount of (personal) data that is being processed by energy providers.
- The energy transition is creating a huge trend in redundancy, with 700,000 fewer workers in the oil sub-sector than in 2016.
- The Energy sector is also increasingly subject to threats of a geopolitical nature, both as a generally disruptive tactic, or sabotage as a weapon of war. The infrastructural risk that the energy sector is exposed to under conflict is also a huge concern, as highlighted by the Nordstream 2 explosion and the siege of the Zaporizhzia nuclear plant in Ukraine.
- The increased targeting of supply chains and subsequent security requirements are especially challenging for the energy sector, where providers have very specific and different supply chains and materials depending on the type of energy they provide.

Rising Heat

- The energy transition is creating huge opportunities and competition, especially in the renewable energy sub-sector. High-value R&D progress and emerging technologies may be sought after by competitors who seek cost-effective means to acquire said technologies to remain competitive.
- The vast vacancies, combined with rapid digitalisation trends raise the increased exposure to (IT) sabotage and the potential for data breaches which the energy sector is subject to. Indeed, the majority of insiders who committed IT sabotage acts conducted them after, or in connection to, their termination or suspension from duties.
- Europol has also highlighted the risk that environmental activists and extremists can have on organisations in the energy sector. Incidents involving environmental extremism have the potential of causing huge damage to public and private property, alongside public order disruption.
- Human error has the potential to be extremely costly, both from a physical damage point of view and from a reputational perspective. The case of the BP oil leaks showed the high damage to machinery and the environment human error can cause, as well as catalysing vast external uproar against an organisation itself.
- Hybrid warfare strategies are growing in effectiveness, and these threats are becoming increasingly complex and common. Targeting energy suppliers and nuclear power plants can freeze a society and increase vulnerability to military operations. Specifically in the area of espionage and nation-state-related sabotage, insiders are often socially engineered through technological efforts such as phishing e-mails. A lack of awareness, training, and robust network countermeasures all contribute to the coercion of insiders by malicious threat actors.

Act Now: Insider Acts are growing in occurrence in the Energy 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.