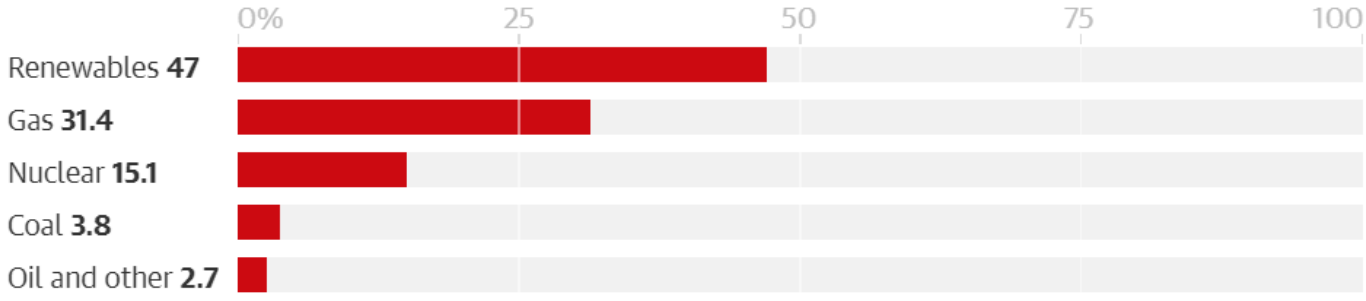
Security Issues in the POWER GENERATION SECTOR

EXECUTIVE SUMMARY

The power generation sector in the UK faces a number of challenges from threat actors including criminals and activists, as well as potential operational disruption from cyber-attacks and terrorist attacks. These threats vary by sub-sector, for example, nuclear power generation experiences more activism from environmental groups opposed to the use of nuclear energy, while renewable solar energy generation is more prone to theft due to the value of equipment used. The high cost of constructing nuclear power stations makes these projects particularly susceptible to financial losses and incidents such as workplace accidents or cyber-attacks can disrupt operations at a high cost per day. This report will outline threats to the power generation sector in detail, and provide recommendations on how G4S can support businesses in mitigating risks.

UK power generation Jan-Apr 2020. Source: Department for Business, Energy and Industrial Strategy



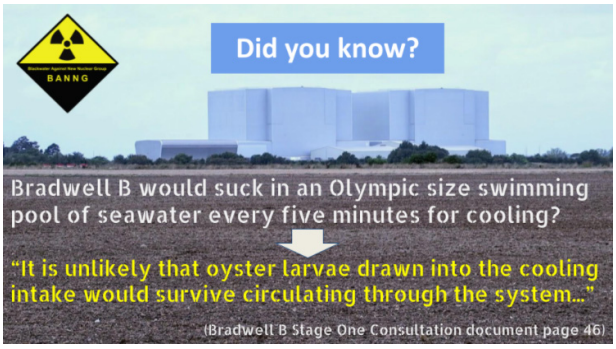
Threat types

CRIME AND TERRORISM

Heightened security measures at nuclear power plants significantly reduce the risk of crime and terrorism. All nuclear power facilities in the UK are protected by members of the Civil Nuclear Constabulary - an armed police force established in 2005 to provide security for nuclear sites and nuclear materials in transit - and private security firms.

PROTESTS & ACTIVISM

The UK is set to increase the number of nuclear power plants after the government identified nuclear power as a way to support its aim of net-zero emissions. In an Energy White Paper published in December 2020, the government unveiled plans to provide up to GBP 385 million in an Advanced Nuclear Fund to support the development of the industry. However, plans to restart nuclear generators which had previously been taken offline have been met with protests by environmental activists. In Scotland, protests have taken place since late 2020 against plans to restart Reactor three at Hunterston B nuclear power station, which was originally shut down in March 2018 for safety reasons. Campaign groups who have called for protests include the Scottish Campaign for Nuclear Disarmament (CND), Friends of the Earth and UN House Scotland. Activists have accused private companies such as those who run the Hunterston B station of acting in their own financial interests, rather than focusing on environmental safety.



Anti-nuclear propaganda posted on 11 January 2021. Source: Facebook

Students protest against climate change in Edinburgh, September 2020. Source: Morningstar Online

Crime such as theft is increasingly likely to target the renewable energy sector, particularly solar farms as solar panels can be easily removed by thieves. These thefts can be both opportunistic and also carried out by organised criminal groups (OCG) who sell these items to fund other criminal activities. (See report on renewable energy for a full overview of crime in this sector).

Anti-nuclear activism is partly attributed to negative media coverage of the issue, as well as historically successful campaigns to halt the use of nuclear power. TV shows such as HBO's Chernobyl and extensive media coverage of the 2011 Fukushima nuclear disaster have highlighted the negative human and environmental consequences from accidents at nuclear power plants. Activist groups on social media to build support for their cause use negative imagery of nuclear power facilities and anti-nuclear propaganda.

CYBER

Power generation remains an attractive target for cybercriminals for a number of reasons. These include, but are not limited to; the potential for disruption and the potential to steal sensitive information, such as from nuclear sites. The negative economic and political consequences of a cyber-attack against these targets is also a factor in their targeting. As the UK moves to increase its nuclear power production, its sites will almost certainly become more attractive targets for attack.

Cyber-attacks can be carried out by state actors, as well as by non-state actors with criminal intent; for example to extract ransom payments or to steal sensitive information with the aim of selling this on the black market. In October 2019, India confirmed that hackers targeted its Kudankulan nuclear power plant. The Nuclear Power Corporation of India Limited confirmed that hackers used malware software designed for data extraction, but said the attack was isolated from the critical internal network. However, according to the Financial Times, cybersecurity experts claim critical information was compromised in the attack. Although no group claimed responsibility for the attack, the software used is linked to a cybercrime group known as the Lazarus group. Closer to home, a cyberattack in 2020 targeted Elexon, a company, which facilitates payments in the UK energy market. Attackers using the REvil/Sodinokibi ransomware stole data, including the passport of the director of customer operations, but the company services were not impacted by the breach.