Security Issues to

ELECTRICITY TRANSMISSION AND DISTRIBUTION

EXECUTIVE SUMMARY

- Security threats for electricity transmission and distribution traditionally stem from crime; however, the sector is also vulnerable to targeted activism and cyberattacks.
- It is plausible that the ongoing COVID-19 pandemic and subsequent negative economic impacts would contribute to an increase in low-level electricity theft in the form of meter tampering, while organised criminal groups will take continue targeting power cables and other valuable metals.
- Protest activity against planned infrastructure such as wind farms and converter stations will likely continue to take place, with environmental groups using social media platforms to garner support for their opposition to projects.
- In addition, critical national infrastructure remains a key target for cyberattacks due to its potential for disruption and its large amounts of customer data. The following report will provide an in-depth analysis of the key threat types and advice on how your business can mitigate the associated risks.

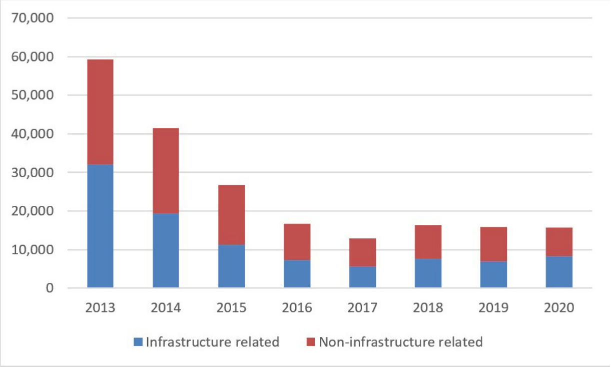
CRIME

The primary type of crime which impacts the electricity transmission sector is electricity theft. It is estimated that energy theft in the UK amounts to approximately GBP 500 million per year, with an average of 25,000 cases of electricity theft annually. This issue is can be customer-specific, such as individuals failing to pay their bills for continued periods of time before then vacating a property. Other customer-led thefts can include tampering with electricity meters or placing magnets on them to alter the reading and thus reduce the overall billing cost. Information on how to tamper with meters is widely available online, with video sharing platforms such as YouTube returning several thousand results showing how to tamper with various types of meter. This type of crime is difficult to detect as it is carried out either in people's homes or by individuals who connect to the meter of a neighbour, often without their knowledge. This is particularly the case if individuals refuse to provide meter readings to their electricity providers or refuse entry to company representatives attempting to take meter readings. Social distancing restrictions currently in place will also make it more difficult to conduct property inspections to determine if a meter has been tampered with.

According to the Office for National Statistics, the negative economic impact of the COVID-19 pandemic has resulted in a 4.9% unemployment rate as of December 2020, with several million more people impacted by reduced working hours and Universal Credit processing delays. Government calls for people to stay at home and school closures during the winter months have seen domestic energy demand increase by up to 10%. Energy regulator Ofgem has put forward plans to allow energy suppliers to increase customer charges in anticipation of a rise in customer debt, essentially receiving higher payments from some customers to make up the shortfall from those who cannot afford to pay. Both the increase in bills combined with potential defaults will almost certainly increase the risk of electricity theft in the immediate to medium term.

Electricity theft is also a common tactic used by narcotics producers and data from 2019 indicates cannabis farms are responsible for up to a quarter of all electricity

Threat types



thefts in the UK. Greater Manchester, West Yorkshire and Merseyside police accounted for a third of all investigations into electricity theft between 2017 and 2019.

The second most common type of crime to impact electricity transmission is the theft of cables from power lines. This involves criminal actors physically removing power lines which they can then sell on the black market. Tactics used by thieves are often crude and dangerous, such as the use of bolt cutters to remove copper cables. According to UK Power, criminal gangs have also previously dug up streets to divert electricity supplies. Due to the risks involved in these acts, large scale metal thefts generally occur as part of organised criminal operations. Indeed, police sources have confirmed to G4S RC that organised criminal groups engage in acts of metal theft as a way to fund other criminal activities. This makes theft from infrastructure and large commercial operations an attractive target due to the higher financial value of items stolen from these sites, as well as the larger number of items that would be found at residential properties. Individuals not linked to organised crime can engage in opportunistic thefts when motivated by financial gain.

PROTESTS & ACTIVISM

Protest activity targeting electricity transmission and distribution can occur in areas where infrastructure projects are planned, or where projects have resulted in environmental damage. It is most common for protests to take place in the planning stage as local residents seek to prevent the construction of infrastructure including transmission towers, wind farms and converter stations in the vicinity of their homes. Protests are prompted by concerns around the negative environmental impacts of these facilities, as well as the potential disruption to tourism. In February 2020, Knockraha Environment Group (KEG) confirmed they had submitted a file containing 1,000 objections to Eirgrid, Ireland's state-owned electric power transmission company, against proposed plans to construct an energy converter facility in the area. As with other environmental groups, KEG has shared its message on social media and has a Facebook page with more than 450 followers. The use of social media platforms to spread awareness of environmental issues and draw support for protest movements is a common tactic used by groups opposed to the construction of infrastructure, but this generally does not translate into large scale demonstrations.

CYBER

The growing use of digital technology in electricity plants increases the risk of cyberattacks targeting critical national infrastructure (CNI). Commercially available operating systems are susceptible to cyberattacks from a wide range of threat actors. This includes state actors and non-state actors such as commercial hackers, script kiddies (low-level hackers who use existing software to carry out cyberattacks), and disgruntled employees who may already have access to targeted operating systems. Interconnected energy networks mean the potential disruption from a cyberattack increases, with the potential to cause disruption to power supplies. More commonly however, cyberattacks are used to steal customer data or by criminal groups demanding a ransom. In March 2020, the European Network of Transmission Operators for Electricity (ENTSO-E) said it had found evidence of a successful cyber intrusion into its network, but did not specify what the attackers had achieved. In 2015 and 2016, cyberattacks targeting power companies in Ukraine disrupted power in parts of Kyiv for up to one hour. More recently in 2020, a cyberattack 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.