Hackers target energy assets for maximum disruption

Cyberattacks on critical energy infrastructure – from pipelines to electricity distribution systems – are becoming more frequent. A culture of transparency and cyber resilience are the sector's best defence, writes *Jennifer Johnson*.

Malign actors are now capable of shutting down the entire US power grid, according to the country's Energy Secretary, Jennifer Granholm. Speaking to CNN's *State of the Union* news programme in June, she stressed that the public and private sectors must work together to neutralise cyber-threats to the country's critical infrastructure.

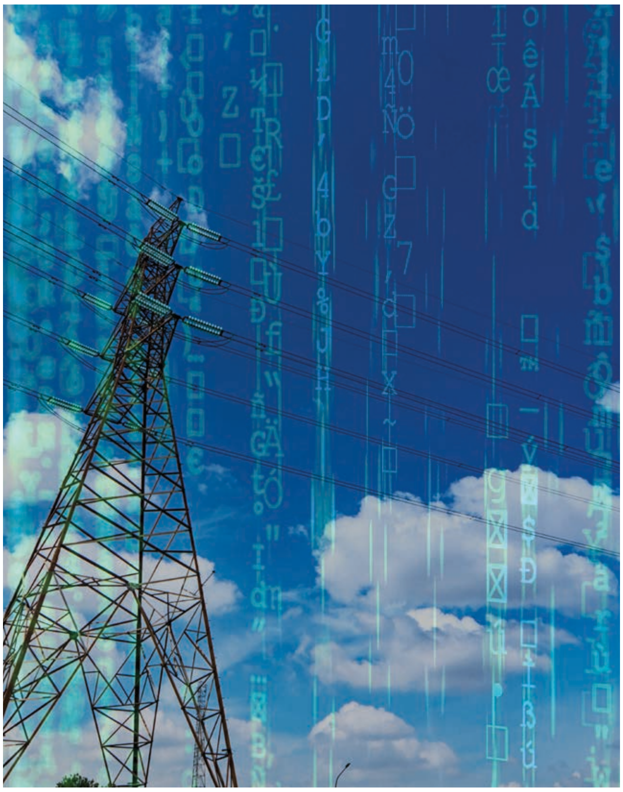
Granholm made the comments in the wake of a highly disruptive cyberattack on the Colonial Pipeline, which stretches from Texas to New York and transports nearly half of all gasoline and jet fuel consumed on the East Coast. It is believed the attack was carried out by a Russian crime group known as DarkSide, though the Kremlin has denied any involvement.

Growing threat

While the Colonial Pipeline incident is perhaps the most high-profile piece of energy infrastructure ever targeted by hackers, it is far from the first. The sector has been well aware of these kinds of threats for years, though many would argue that not enough has been done to shore up key assets. The first known attack on a power grid took place in December 2015 in Ukraine, where hackers remotely accessed computer systems to switch off substations. As a result, 225,000 people lost power for several hours.

Several weeks later, the US cyber intelligence firm iSight Partners attributed the attack to a Russian hacking group known as Sandworm. It was reported at the time that the group was operating in alignment with the Russian state, if not working for them directly. In the aftermath of the hack, Ukraine's grid operator dispatched staff to control breakers directly. But as grids become more digitalised, this kind of manual intervention may become more difficult.

The World Economic Forum's *Global Risk Report 2020* said that cyberattacks are among the top 10 global risks in terms of likelihood and impact. For the electricity sector in particular, these threats are significant and intensifying. However, it remains tricky to properly evaluate the risks and knock-on effects of cyberattacks in the energy sector, in part because there's so little available data about them.



In a ransomware attack, hackers will trick unsuspecting staff into opening an email and clicking on a link or attachment. Computer servers are then infected with malware that encrypts their data.

In a report into cyber resilience released earlier this year, the International Energy Agency (IEA) wrote that 'many incidents may not be reported at all – even to regulators or other authorities'.

While regulators in many countries ask companies to come forward following a cyberattack, there is an obvious incentive for not doing so. Namely, that disclosing a hack could hurt a company's credibility and possibly its share price. As the number of high-profile cybercrimes grows, regulators will no doubt levy more serious reporting obligations on private companies. In the aftermath of the Colonial Pipeline attack, the US Department of Homeland Security (DHS) mandated that pipeline operators report cybersecurity incidents within 12 hours. Pipeline owners and operators must also designate a cybersecurity coordinator who is available to consult with the relevant government departments 24 hours a day. The directive will apply to around 100 companies considered to have the most critical pipelines in the United States.

Who is behind cybercrime?

According to FireEye, a California-based cybersecurity firm, the energy industry faces threats from two types of malicious actor: advanced persistent threat (APT) groups and so-called 'hacktivists'. The former attempt to steal information for the purpose of assisting a sponsoring government with national and economic security issues. In a sector-specific threat intelligence report, FireEye stated that data thefts will likely be centred on information related to natural resource exploration and energy deals.

Hacktivists, on the other hand, are more likely to target companies to attract attention to a cause or make a political statement. This appears to have been the motivation behind a string of cyberattacks that took place in Saudi Arabia in early 2017. In January, computer systems went down at two major petrochemical firms, Tasnee and the Sadara Chemical Company, a joint venture between Saudi Aramco and Dow Chemical.

The *New York Times* reported that within minutes of the Tasnee attack, hackers wiped the company's computers and installed an image of a child who had perished in the Syrian civil war.

Cybersecurity researchers believed the people behind the incident wanted to inflict lasting harm on the petrochemical companies and send a political message. However, the majority of attacks on the energy sector appear to have been carried out by APT groups, or simply cyber-criminal gangs motivated by the prospect of earning money. The Colonial Pipeline incident is an example of one such 'ransomware' attack. The pipeline's operator authorised a ransom payment of $4.4mn in cryptocurrency to the hackers after the attack.

For hackers looking to extract a quick ransom, energy companies make an attractive target, as they provide critical services that operators will be keen to resume as fast as possible. It only took a few hours for the Colonial Pipeline bosses to pay a ransom in hard-to-trace digital currency to the hackers that targeted their firm.

In a typical ransomware attack, hackers will often trick unsuspecting staff members into opening an email and clicking on a link or attachment. Computer servers are then infected with malware that encrypts their data (transforming it into unintelligible code or symbols) and locks the computer systems. To obtain a 'decryption' key and recover the information, victims must pay the hackers a ransom.

Critical vulnerabilities

In its *Cyber Resilience* report, the IEA states that cybersecurity 'needs to be integrated into the culture of the organisation…rather than being considered as a separate, technical issue'. The agency maintains that cyber resilience is a combination of 'preventive and corrective measures building on lessons learned after a cyberattack' – which makes transparent reporting a critical part of preventing future attacks. It's also important that staff members are made fully aware of what cyber threats look like, so they don't unwittingly put their employers at risk.

It is believed that a 'spear-phishing' attack, in which individuals are sent malicious but believable scam messages, brought down another US pipeline last year. The facility in question was not named, though the Department of Homeland Security did issue a briefing following the incident.

Once the perpetrators gained access to the IT systems at the affected natural gas compression facility, it unleashed ransomware that led the company to 'lose sight' of some of its digital systems. As a result, it had to shut down its pipeline network for two days. The DHS said the attack was more severe than it might have been because the company had not been adequately prepared for it.

> *For hackers looking to extract a quick ransom, energy companies make an attractive target as they provide critical services that operators will be keen to resume as fast as possible*

As more 'smart' technologies are integrated into energy networks, the number of sensors and connections also grows, giving hackers greater access to key infrastructure and services. In the past two years, the security firm Darktrace says there has been an increase in cyberattacks directed at a variety of critical industries, including electricity distribution.

The cross-border nature of hacking means that no company or organisation is truly safe from these kinds of threats. For instance, India's largest nuclear power station was targeted in 2019, possibly by North Korean hackers attempting cyber espionage.

Bringing down a critical energy asset is hugely disruptive, and the connectedness of the modern energy system means that there are more opportunities to gain access to infrastructure than ever before. Before the internet age, shutting down a pipeline meant physically obstructing the flow of oil. Now breaking and entering a site is as easy as sending a fraudulent email from thousands of miles away.