Energy Insight: Cybersecurity in the energy sector

Highlights

The following Energy Insight provides an overview of the topic of cybersecurity. It covers:

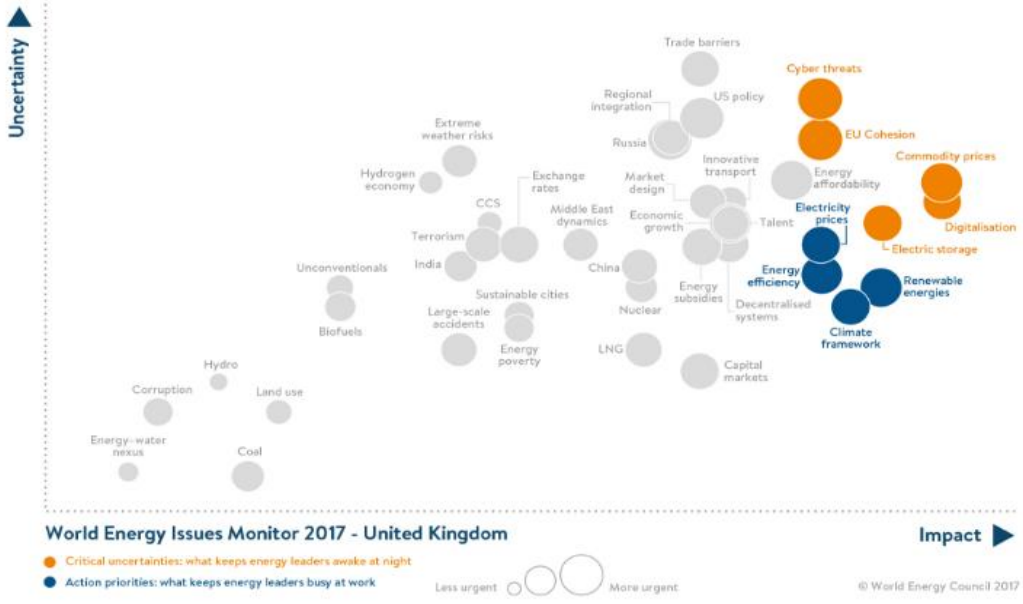
- The history of cybersecurity
- Legislation
- Cybersecurity in the oil and gas sector
- Cybersecurity in the nuclear energy sector
- Cybersecurity for the grid and smart systems

Introduction: A history of cybersecurity

Cyber security refers to technologies, processes and controls that are designed to protect systems, networks, devices and data from attacks and unauthorised access.

The first instance where people had to respond to a cybersecurity attack was when the first computer worm was created in the late 1980s-early 1990s. This shut down most of the internet and laid the foundations for the types of security problems we have had since. In the 1990s the first viruses were introduced that infected millions of computers which led to the development of antivirus software. In the late 2000s cyber-attacks became more targeted when information was stolen from millions of payment cards. Fast forward to the present day and cybercrime is highly sophisticated and hard to prevent. Companies have had to put strategies into place to deal with cybercrime and build up resilience to these attacks.

With increased digitisation cybersecurity has become of paramount importance and cyber-attacks are regarded as a high risk to the energy sector. In 2017 research was conducted into world energy issues across 90 countries. The UK was found to have critical concerns about cybersecurity along with Japan and Singapore. This is due to increased digitisation surrounding the expansion in solar and the roll out of smart meters.



Source: World energy issues monitor 2017, World Energy Council, 2017

Legislation

The UK government set out a National Cyber Security Strategy 2016 to 2021 to ensure Britain has a resilient and secure cyberspace. A total of £1.9 billion will be spent from 2016-2021 in order to significantly improve the UK's cybersecurity. To make this happen three objectives will be put into place:

1. Defend: Ensuring the UK has the means to defend itself against and respond to cyber attacks
2. Deter: Ensuring the UK has the means to investigate and prosecute those who carry out cyber threats.
3. Develop: Ensuring the UK has the knowledge and expertise to conquer threats and future cyber security challenges

A National Cyber Security Centre (NCSC) has been created to provide leadership and share knowledge on national cyber security issues.

In November 2016 the "Clean Energy for all Europeans" legislative package was launched by the European Commission. This package aimed to facilitate the move to a more decentralised energy system, the roll-out of smart meters being an aspect of this. Part of this package contained an Electricity Directive which aimed to include GDPR guidelines relating to the implementation and function of smart meters.

In February 2017 the "Civil Nuclear Cyber Security Strategy" policy paper was published by BEIS. This strategy supports the government by ensuring the civil nuclear sector is resilient and able to defend against cyber threats.

In March 2017 the Energy Expert Cyber Security Platform (EECSP) published a "Cyber Security in the Energy Sector" report. The EECSP provides the European Commission with recommendations and guidance in the energy sector. The report covers the work of the EECSP towards the development of the European Commission's energy cyber security strategy which will complement the NIS Directive and GDPR. The Expert Group recommended four key strategic priorities to the European Commission. These were:

1. Have a threat and risk management system in place
2. Create an effective cyber incident response framework
3. Improve the energy sector's resilience to cyber attacks
4. Expand the resources and skills needed to address cyber security

The Networks and Information (NIS) Directive is an EU directive that came into effect in August 2016. It aims to improve the strength and security of networks across the European Union. The UK implemented NIS regulations into its domestic legislation on 20 April 2018. The regulations will prepare electricity, transport, water, energy, health and digital sectors for cyber threats and is part of the UK's National Cyber Security Strategy.

The new General Data Protection Regulation (GDPR) was enforced on the 25 May 2018. It replaces the Data protection Directive 95/46 EC and was designed so all companies in the EU follow one set of data protection rules. It aims to change the way organisations approach data privacy and to protect all EU citizens data privacy.

Cybersecurity: oil and gas

There are many areas in the oil and gas sector that could get struck by a cybersecurity attack, these include, but are not limited to lack of training and awareness of cybersecurity issues among employees, vulnerable and outdated systems and using vulnerable IT products in the production environment.

There are three major stages in oil and gas production that are particularly vulnerable to cyber-attacks. These are exploration, development and production and abandonment. Figure 2. Takes various aspects of oil and gas production and places them on a scale of vulnerability to cyber-attack versus the severity of cyber-attack. Geophysical surveys and seismic imaging have a fairly low risk whereas production and development drilling are high risk.

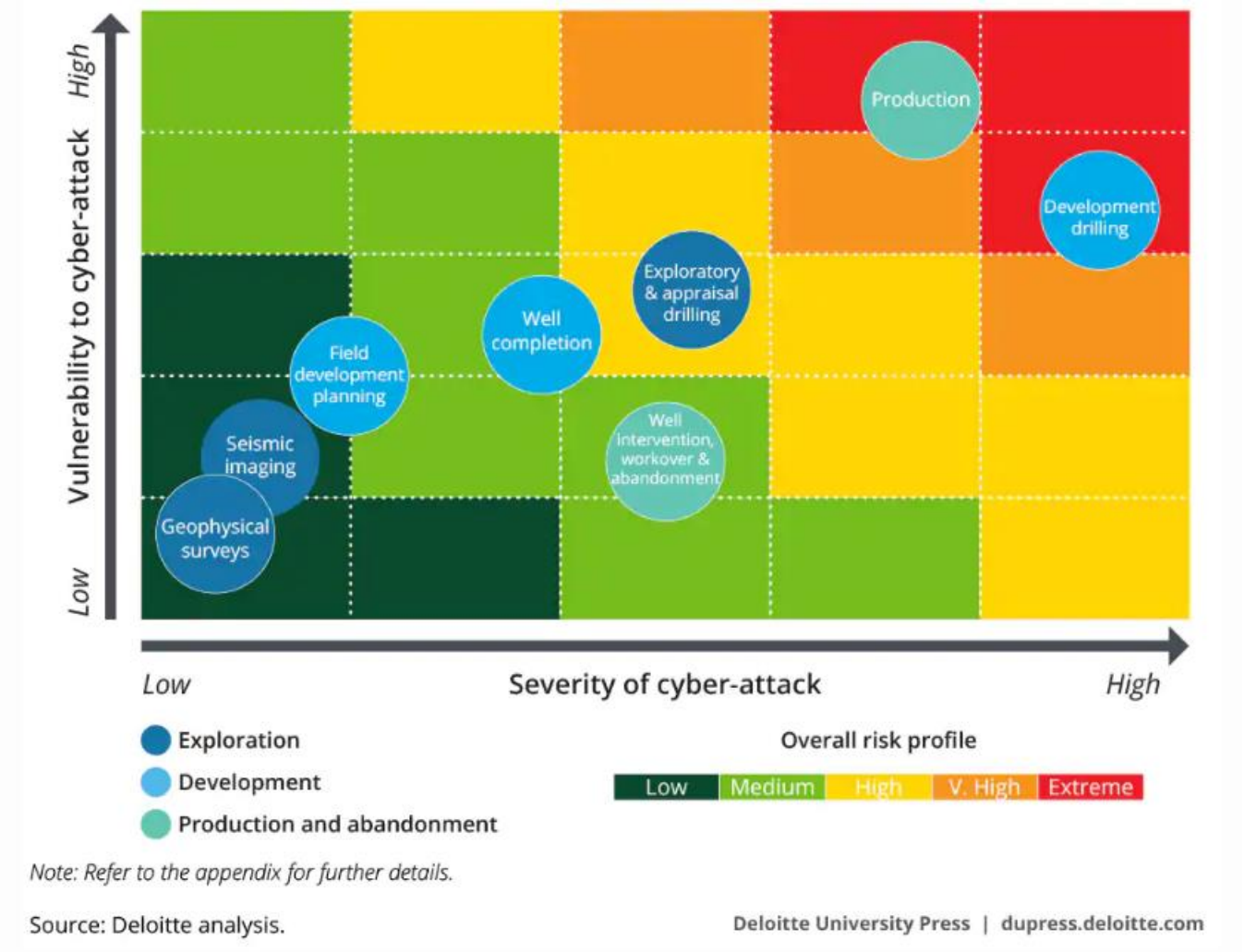


Figure 2. Cyber vulnerability/severity matrix by upstream operations, Deloitte analysis, 2017

There have been a few noteworthy cybersecurity attacks in recent years. In 2012, Shamoon, a computer virus that wiped data from master boot records, disabled thousands of computers in Middle Eastern oil and gas companies. Saudi Aramco was hacked in 2012. A computer virus spread through personal workstations which forced Saudi Aramco to isolate its production systems from them. It was not clear whether this was a state sponsored attack, or a virus found online. In 2014 there was an attack on the Norwegian oil industry which led to the hacking using Trojan horse and phishing campaigns of exploration data for more than 50 oil and gas companies.

Many services have been set up to help oil and gas companies protect their assets from cyber-attacks. For example, the data service provider Dataminr helps oil and gas companies by monitoring and protecting their assets by filtering and processing social media (mainly Twitter).

Cybersecurity: nuclear

Little thought was given to cybersecurity in the nuclear industry as it was developed when computers were in their initial stages. Nuclear power plants are now more exposed to cyber attacks due to increased use of digital systems, use of bespoke systems, vulnerabilities in the supply chain and new nuclear plant models that operate solely on a digital system.

In 2010 the Stuxnet worm interfered with the nuclear programme in Iran. Stuxnet entered the computer system via a USB stick which was inserted into a computer attached to the network at the nuclear plant. Stuxnet then searched for software that controlled the centrifuges and seized them, so it could control them itself. It made the centrifuges spin extremely fast before returning to normal about 15 minutes later. After about a month the centrifuges were slowed down for a period of time which was repeated for several months. Infected machines began to disintegrate due to the excessive speeds they were spinning at leading to Iran decommissioning about one fifth of centrifuges at Natanz.

A dataset has recently been launched which ranks countries by the strength of their cyber security (theft and sabotage) at nuclear facilities. The UK is tied in 11th place in the ranking, behind countries such as Australia, Switzerland and Canada who occupy 1st, 2nd and 3rd spots respectively. The UK has a high number of nuclear materials across many sights which contribute to adverse security conditions. To improve our ranking more frequent personnel vetting procedures could be undertaken to lessen the threat of insider cyber-attacks.

Cybersecurity: the grid and smart systems

63% of utility directors from around the world believe that in the next five years their country faces at least a moderate risk of electricity supply disruption from a cyber-attack on electricity grids, according to a recent report by Accenture. The grid is vulnerable because there are so many interconnected parts across vast spaces. The infrastructure is required to operate for up to a decade, so the technological systems are upgraded less frequently.

In 2016 hackers targeted an electric transmission station in Ukraine, north of Kiev. The power outage lasted around an hour and approximately one fifth of Kiev's power was lost. This was the second year in a row that a cyber-attack was carried out on Ukraine. The name of the virus was Industroyer and was built specifically to target industrial control systems. This is the second known virus specifically built to disrupt industrial control systems (the first virus: Stuxnet, interfered with the nuclear programme in Iran). These viruses use standardised infrastructure communication protocols to target electricity substations and circuit breakers.

Hackers are becoming more sophisticated in their attempts to disrupt the grid. Older power plants have managed to avoid cyber-attacks as they have not been connected to the internet, however, the grid is moving towards a more distributed model and the energy industry is currently experiencing a rapid increase of digitalisation. This can be seen in the form of devices on the smart grid as well as prosumers exporting and importing their own electricity to the grid. By 2020 smart meters will be installed in every home. This is one obvious target for cyber-attacks but the chief technology officer

of the DCC, the Capita-run body set up to handle the data, states that the data will be safe as sensitive data is not held on customers and the systems will not be connected to the internet.

Research into grid security has been undertaken and two suggestions have been made to make it more robust. One suggestion is to add more equipment that can take over when an attack prevents a power station of transmission line from working, however, this is costly. A second approach is to analyse the risks in the systems and develop techniques that help prevent, detect and respond to attacks. To protect the smart grid cybersecurity measures that can provide real time performance and continuous operations should be employed. Modern and secure Wi-Fi access and encrypted cloud storage should also be implemented to make sure customer's data is secure from hacking. To safeguard the grid in the future all companies must play a part and make sure their security systems are up-to-date.

Further Reading

Protecting the connected barrels: cybersecurity for oil and gas. Deloitte, 2017.

Cyber security in oil and gas. PwC, 2017

Cyber security in the nuclear industry: Growing threats and evolving practices. PwC, 2017

World energy issues monitor 2017. World Energy Council, 2017

World energy issues monitor 2018. World Energy Council, 2018

Cyber security in the energy sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative acts for the Energy Sector. EECSP, 2017

Cybersecurity for the energy sector: Everybody's war? Siemens, 2017

Cyber Security of UK infrastructure. Parliamentary Office of Science and Technology, May 2 2017

There is a UK government page dedicated to cybersecurity policies and information.