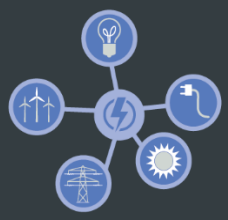
Bird & Bird ATMD

Cybersecurity & Singapore

Risks for an Increasingly Digitalised Energy Sector

July 2019



*The energy sector is becoming increasingly digitalised and companies in this sector should consider how digitalisation affects them. This sixth article in our **Cybersecurity & Singapore** series highlights the impact of digitising energy sector, in respect of cybersecurity incidents and risks.*

The introduction of the open electricity market in 2018 enables households to have a choice of retailer from whom they can purchase electricity. Conseque ntly, retailers will have records of their customer's personal data. As many households will sign up to purchase electricity from the various companies, each company will have records of a vast amount of personal data of its customers. These energy retailers should consider having measures in place (such as encrypting the data or having a firewall) to ensure that such personal data is protected, as required under the Personal Data Protection Act 2012, and to prevent third parties from having "unauthorised access" to their customer data.

Entities in the energy sector face significant risks of cyberattacks as rapid digitalisation of the sector brings about increased electronic exchange and access to information and systems. The Cybersecurity Act 2018 (No. 9 of 2018) ("**Cybersecurity Act**") was passed in early 2018. The Cybersecurity Act is concerned with critical information infrastructure ("**CII**") and the energy sector is one of the sectors identified as CII. Under the Cybersecurity Act, essential services include the distribution, transmission and generation of electricity. A disruption to an essential service is regarded to be a cybersecurity threat under the Cybersecurity Act. The Commissioner has very wide ranging powers under the Cybersecurity Act to investigate cybersecurity threats and, inter alia, eliminate cybersecurity threats. Entities in the energy sector which are regarded as CII thus have to put measures in place to assess how secure their computer or computer systems are including conducting an audit at least once every 2 years to determine if the CII complies with the Cybersecurity Act and conducting a cybersecurity risk assessment at least on an annual basis.

Entities in the energy sector also face cybersecurity risks when they are involved in merger and acquisition transactions. In the event that a vendor intends to dispose of the shares or the assets of a company in the energy sector, information relating to the target, including sensitive information, may be uploaded onto the virtual data room. It would be prudent for the vendor to appoint a virtual data room service provider whose virtual data rooms are sufficiently secure to minimise the risk of unauthorised access to the target company's information if there were to be a cyber attack on such service provider. The vendor may also consider not uploading documents containing sensitive information onto virtual data rooms.

The European Cybersecurity Agency, European Union Agency for Network and Information Security ("**ENISA**") is of the view that a lot can be done to address the challenges identified for the energy sector at the EU level including the following measures[1]:

- Harmonising the approach to cybersecurity across EU Member States to reduce the risk of weak links in the increasingly interconnected European grid.
- Developing a common understanding of the cybersecurity threat landscape.
- Developing a common cyber-response framework that helps operators to identify what is needed in order to protect themselves from cyber-attacks.

Singapore and ASEAN can consider taking the same approach by harmonising their cybersecurity legislation. The various states can identify and have a common

[1] *https://setis.ec.europa.eu/system/files/setis_magazine_17_digitalisation.pdf*

understanding of the threats in the cybersecurity space that affect companies in the energy sector and develop a common framework and this is in progress as the third ASEAN Ministerial Conference on Cybersecurity has "agreed that there is a need for a formal ASEAN cybersecurity mechanism to consider and to decide on inter-related cyber diplomacy, policy and operational issues[2]".

Authors

Ken Cheung
Partner

Tel: +65 6428 9893
ken.cheung@twobirds.com

Mark Louis Low
Senior Associate

Tel: +65 6428 9473
marklouis.low@twobirds.com

Contact us

For queries or more information, please do not hesitate to contact any member of the Energy & Utilities team.

Ken Cheung
Partner

Tel: +65 6428 9893
ken.cheung@twobirds.com

Sandra Seah
Joint Managing Partner

Tel: +65 6428 9429
sandra.seah@twobirds.com

Mark Louis Low
Senior Associate

Tel: +65 6428 9473
marklouis.low@twobirds.com

Eef Gerard Van Emmerik
Associate

Tel: +65 6428 9474
eefgerard.vanemmerik@twobirds.com

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Berlin & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw

1809187.7

2 https://www.csa.gov.sg/news/press-releases/amcc-2018