Cyber Security Risk for Energy sector

Smart decisions. Lasting value.

INTRODUCTION

Digitisation of data mobility in the following four key energy sectors is undergoing a transformational change in social, technological and economic paradigms:

- Electric Energy transmission
- Oil and Gas supply
- Wind energy
- Renewable energy

Sectors are being disrupted, with new technology and digitisation. The winners are likely to be those that can truly understand the impact and timing of disruption and seize the right emerging opportunities.

Digitisation in energy sector is growing vertically where data mobility is the key factor for off shore and onshore organisations, while cyber threat for data transmission is increased for remote access users.

DIGITAL TRANSFORMATION

Digital transformation brings significant revolution in energy sectors while increasing the risk of securing information from cyber crime. It is swiftly lowering the costs for mobility and other operational activities. The underlining question is whether organisations are secure from cyber-attacks due to the open data access of mobile devices? It is crucial that the process of digital transformation and managing Cyber Security should be approached parallelly.

CYBER SECURITY

The Oil and Gas sector, today is highly dependant on technology and Cyber Security threat, posing a significant risk. This emphasizes the need to adapt and upgrade technology to manage potential threats. Data privacy and security is a risk that needs to be managed as there is an exponential increase of flow in information.

Digitization and mobility are the key focus areas for energy companies, due to multiple locations and countries they operate in. This results to higher risk for cyber-attacks and the need to educate employees and stakeholders is vital.

As large energy companies operate in multiple countries and jurisdictions it is important to educate and raise awareness of respective cyber regulations specific to those countries. This would ascertain whether they are in compliance with the applicable regulations and standards. Monitoring and education should be an ongoing process to control the risks.

It is the technology department that needs to initiate a deep dive analysis of the Cyber Risk of the overall organization. Preparing an overall risk analysis report of all the divisions and departments of the organisation.

Cyber risk measure and digital transformation should be conducted parallelly to identify a remedial tool.

With the advent of energy technology applications along with integrating data analytics with numerous suppliers, it is crucial that regular audit for user integrity with data security should be conducted.

To minimise risk, organisations may require implementing the following fundamental actions:

- Board-level discussion and review for potential risk for Information security.
- Spread awareness and educate employees for potential risks and their responsibility.
- Identify risk of reputation of the organization on cyber threats.
- New challenges against rise with the Internet of Things (IoT).
- Develop skilled cyber workforce in-house for evolving threats.
- Potential financial impact of breach needs to be examined.
- Organization has to developed agility to face potential risks of Cyber attack

Crowe UAE
Level 21, Prism Tower, Business Bay
Dubai, UAE
+971 4 447 3951
www.crowe.ae

Contact

Zayd Maniar
ILP
zayd.maniar@crowe.ae
+971 50 645 8693

Binit Shah
Partner
binit.shah@crowe.ae
+971 55 212 9830