





# Introduction

Digitisation is changing the dynamics of accessibility, productivity and sustainability of the energy system. In the coming years, digital technologies will make the energy sector more connected, intelligent and efficient, so that the inherent infrastructure could smartly detect who needs 'how much' energy and 'in what capacity'. Rapid transformation in digital assets, in addition to fast changing dynamics of the energy sector, will present key stakeholders with complex decisions to safely and sustainably produce and manage sources of energy, especially when they are built upon the foundation of a long-standing physical infrastructure.

## Key trends

- Blockchain**  
 The implementation of Blockchain technology brings in many advantages. It enables an ease of doing business, and, at the same time, helps maintain compliance (with abilities to reduce potential fraud), and maintain integrity of data and authenticity of transactions across business lines (this includes efficient energy trading, reliable financial transactions, compliance to regulatory requirements and integration of interoperable applications and infrastructure).
- Internet of Things (IoT)**  
 Oil and gas companies typically have numerous remote assets that require efficient operation, communication and monitoring. IoT is making it a lot easier to collect critical information, which then helps the business make more informed decisions.
- Artificial Intelligence (AI) and Machine Learning (ML)**  
 The oil and gas industry can use AI and ML data science and analytics to solve complex data structures and formats used for oil and gas exploration and production, and thereby, create new exploration opportunities.
- Big data and analytics**  
 Digitisation helps collate data on a single platform. Business Intelligence (BI) analysts help organisations in setting predictive metrics that ultimately lead organisations into taking informed decisions. This data, when analysed and correlated, has the capability to detect and transmit a variety of information, such as breakdowns, preventive maintenance, non-standard movements, leaks, corrosion, and additionally, alerts the concerned based on the preset rules and algorithms.
- 3D and 4D Printing**  
 This technology supports and enables an interactive process to create and manufacture plant parts and materials, while also reducing the use of complex components, weight, and manufacturing costs. This will prove beneficial for the energy sector as it is a machinery-intensive industry.
- Cloud**  
 Oil and gas companies are moving to cloud computing technologies to transform their back-office systems, operations and to integrate their core products and on premise solutions to provide a consistent platform of offerings.

## Threat landscape

The energy sector has become more digitised, adding to the complexity of architectures, integrations, operations and maintenance. Critical control systems, that were once completely isolated, are now part of the organisational network and can be infiltrated from numerous access points. The high economic value of oil and gas facilities globally, and the inherent issues and gaps within the industry's underlying infrastructure, platforms and applications, provide threat vectors with a great incentive to attack.

In a report, 68% of oil and gas companies surveyed, admitted that their operations have been compromised at least once in the past year.

In a survey conducted by Ponemon Institute, only 41% of businesses monitor their infrastructure continually to spot, prioritise and deal with threats.

In the same survey (conducted by Ponemon), they found that only 45% of companies surveyed believe they have the necessary internal expertise to manage cybersecurity threats in the modern OT environment.

## Major security risks

Risks	Reasons
Use of vulnerable IT products	Many products and applications deployed within the network and production environment are not properly assessed.
Lack of security awareness	There is a lack of cybersecurity awareness and training among employees. Board-level attention is still a concern as well. A recent survey conducted by Sophos, states that at least 90% of Indian organisations believe that their biggest challenge is to improve cyber-awareness training.
Weak security culture among vendors, suppliers and contractors	Contractual oversight of obligations and security posture amongst third-parties is a key concern
Security concerns arising due to the rise of IoT	Sensors, devices, systems and embedded applications are either, increasingly being connected to corporate networks, or using the internet and cellular networks to communicate. This gives rise to inherent vulnerabilities with regard to compatibility, integration and secure configurations compliance.
Ineffective SOC or incident monitoring	Faster adoption of cloud models (such as SaaS, PaaS) relies on vendor controls and assurance reports, and often neglects some service reviews and critical incident monitoring compliances. Additionally, it has been found that non-business critical applications, which have weak controls and are not typically monitored, are sometimes bundled in, and could lead to potential compromises.
Coping with newer laws and regulations	Changes to the existing risk landscape, controls and reporting are time-consuming and could potentially lead to skipping key requirements under the governing laws.

## Our solutions

The energy industry has global economic value and can have an impact across other sectors. Therefore, it is imperative that the information risk strategy encompasses the entire supply chain; right from exploration and drilling, to the retail site, and appropriately covers every point in between.



Sources  
<https://www.techesscyber.com/2018/08/top-cybersecurity-vulnerabilities-for-oil-and-gas/>  
<http://www.turn-keytechnologies.com/blog/network-solutions/why-the-oil-and-gas-industry-is-vulnerable-to-security-threats>  
[http://economicstimes.indiatimes.com/articleshow/71854243.cms?utm\\_source=contentofinterest&utm\\_medium=text&utm\\_campaign=cpsst](http://economicstimes.indiatimes.com/articleshow/71854243.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cpsst)