The hydrocarbons sector is increasingly turning to digital solutions to monitor, predict and optimise operations, enabling companies to better insulate themselves against market volatility. The process of digitalisation will create significant vulnerabilities in terms of cybersecurity and data privacy. O&G companies are particularly exposed, and it will take government and industry cooperation to mitigate the risks.

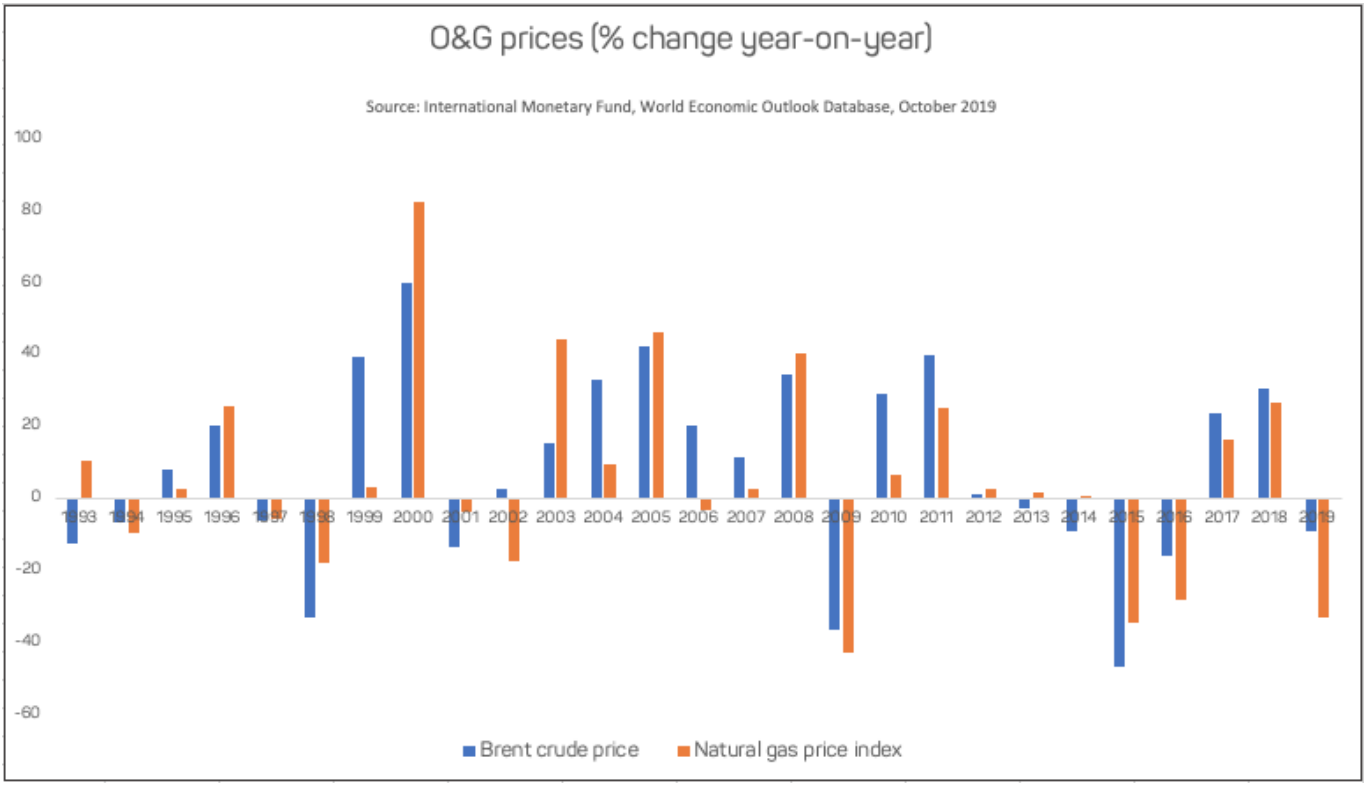
Technology enabling companies to "do more with less"

Integrating digital technology into upstream and downstream operations has become a central pillar of corporate strategy across the O&G industry. Adopting digital solutions and leveraging technology to monitor and predict operations allows companies to boost efficiencies, optimise performance and improve working conditions, while using fewer resources. According to a report by McKinsey&Company, using digital technologies can not only create more value from existing operations, but also potentially reduce capital expenditure by 20% and operating expenditure by 3-5%.[1]

Market volatility accelerating digitalisation

The adoption of innovative technology in the O&G sector, particularly upstream, is nothing new; however the urgency with which companies are turning to digital applications has accelerated, underpinned largely by companies seeking ways to better insulate themselves against market volatility.

The downturn registered across global commodity markets in 2014, in particular, provided a short but significant shock to players across the heavy industries and highlighted the need for companies to develop resilience. While the sector has long-experienced boom and bust cycles, the magnitude of downturns has grown since 2008.



O&G price volatility is an issue for GCC countries in particular, given their continued reliance on hydrocarbons revenue for economic growth and government spending, despite the adoption of national economic diversification programmes. As such, implementing cost-cutting and boosting efficiencies are of elevated importance for national oil companies (NOCs) and, by extension, governments across the region.

Persistent market volatility, along with a number of other factors, including the global shift towards decarbonisation; increased environment, health and safety accountability; rising labour constraints; and an ageing global asset base will ensure that digital transformation continues at pace. In addition to these push factors, advances in technology is an important trend that is enabling digitalisation.

Technology adoption in line with Industry 4.0 transition

Cloud computing, big data, blockchain, AI, robotics, 3D printing and the Industrial Internet of Things, among other technologies, are enabling the wider collection and analysis of data, increased automation and boosted connectivity across O&G business operations. This shift towards increased

interconnectivity, automation, machine learning, and real-time data aligns with the wider pan-industry global trend of Industry 4.0. O&G companies operating across the GCC provide useful examples of digital transformation.

The adoption of digital solutions by NOCs in the GCC is growing increasingly prevalent. The use of technologies like blockchain, robotics, smart sensors, wearable technologies and big data is allowing NOCs to optimise operations and boost profitability in various ways. For example, Abu Dhabi National Oil Company is using Predictive Asset Analytics to prevent equipment failures, while Saudi Aramco is deploying robotics to improve oil recovery efforts in remote areas. Petroleum Development Oman and Fujairah Oil Industry Zone, meanwhile, are developing digital platforms and blockchain technology to enable greater efficiency within the workforce.

Company	Activity
Petroleum Development Oman	PDO, in a joint venture between the government, Shell, Total and Partex, is collaborating on an industrial mobility platform
	The platform is being rolled out across PDO's upstream operations in Oman and will reportedly make fieldworkers 20% more efficient
Fujairah Oil Industry Zone	FOIZ, in a partnership with Platts, is utilising blockchain to track oil storage data in the UAE
	The technology allows traders to securely submit weekly oil inventory data to the regulator (FEDCom)
	It alleviates the need for the regulator to undertake manual validation and aggregation of each terminal operator's numbers, reducing the scope for human error
Saudi Aramco	Aramco has partnered with German software multinational SAP to establish a cloud-based digital marketplace for its buyers and suppliers (the SAP Cloud Hub)
	The move forms part of Saudi Aramco's digital transformation strategy
	The strategy also includes the use of robots and self-guided autonomous devices in remote regions, and the installation of smart sensors with advanced analytical capabilities
Kuwait Petroleum Corporation	KPC is undertaking the "Kuwait Integrated Digital Oil Field" project (KwIDF). The plan involves four different fields in the country and four digital field pilot projects
	The rollout and expansion of phase 1 covered nearly 1,200 wells and began in 2015 with completion in 2017. Phase 2 of KwIDF began in 2018.
Abu Dhabi National Oil Company	Digital technology forms a key component of ADNOC's integrated 2030 Strategy
	Developed by Schneider Electric, ADNOC's "Panorama Digital Command Centre" establishes a single home for all the company's data across the entire value chain. The Panorama centre reportedly enables savings of $60m-$100m through optimised operations.
	IT multinational AVEVA's Predictive Asset Analytics solution is being deployed by ADNOC to reduce unscheduled downtime and prevent equipment failures.

Cyber security & data privacy issues to the fore

Greater interconnectivity between computing devices, personnel and equipment and the exponential increase in the amount of data that is generated will create significant vulnerabilities in terms of cyber security and data privacy. This creates major financial, environmental and social risks across all aspects of the O&G value chain. Hydrocarbon firms are particularly exposed to these risks for several reasons:

Capital-intensive projects: The inherently risky and capital-intensive nature of developing hydrocarbons, notably in the exploration and production (E&P) phase means that minor data breaches

or cyberattacks could be extremely costly. For example, a data breach or cyberattack could result in a production shutdown, environmental destruction or loss of life, potentially causing significant financial and reputational damage to the company. Furthermore, the long timeframes and high costs associated with E&P projects means that the capital at stake per data breach or hack is extremely high.

National security targets: The impact that cyberattacks on national oil companies can have on the wider economy and national security make them an attractive target, whether that be through national defence policy, corporate espionage or terrorist activity. The hydrocarbon companies in the GCC provide a pertinent example in this regard, with the attacks on Saudi Aramco's oil assets being the most recent example.

Exposure to frontier markets: O&G companies, as with other extractive industries, have a heavy exposure to frontier markets, due to a country's resource base being more important to attracting investment than the business environment. This can mean that O&G operations are undertaken in highly unstable and volatile regions where the cyber threat from organised crime groups, domestic extremist groups, regional militants and international terrorist organisations is high.

Furthermore, regulatory frameworks in frontier markets are generally less developed to protect against digital vulnerabilities. While this is an issue across global markets, frontier markets with typically weaker levels of governance, limited monitoring mechanisms and an absence of regulations are particularly prone to cyber-related crime.

Industry fragmentation: The supply chain of the O&G sector is highly fragmented and the resulting sharing of data between many different entities raises the risk of breaches. For example, E&P companies frequently work with a number of contractors, including oilfield services companies, and engineering, procurement and construction firms. Joint ventures with other entities (private players, state-owned enterprises) are also formed in order to develop resources.

An inability to standardise systems and consolidate data across operations exacerbates the issue of fragmentation, particularly given the wide geographic distribution and remote nature of operations for many firms. Italian oil and gas industry contractor Saipem, which operates in over 60 countries, suffered a cyberattack in December 2018 which impacted its servers based in the Middle East, India, the UK and Italy.

Government & industry cooperation essential to mitigating risk

While there is no definitive solution to mitigating data-related risks in the O&G sector, it is clear that firms will dedicate increased resources into cybersecurity over the coming years. Increased investment into digital protection against breaches or attacks, such as physical asset protection and firewalls, will be a central aspect of this investment. Non-digital investments will also be important, including development of more secure employee work processes and access procedures. Furthermore, companies are increasingly adopting emergency preparedness plans to include data vulnerabilities in the event of a barrier failure.

Governments will also have a role to play in terms of ensuring concerns over data privacy, usage and security are addressed in regulation. Frequent dialogue and cooperation with industry players on best practices relating to data usage and sharing will form a key component of this.

Georgina Hayden is an energy consultant and co-founder of research and analysis firm, North Shore Analysis. She has a special interest in the low-carbon economy, and the challenges and opportunities facing stakeholders operating in an increasingly digitalised, decarbonised and decentralised energy system. Before that, she was Head of Power & Renewables Research at Fitch Solutions. She holds a master's degree in Geopolitics, Territory and Security from King's College London.

Sources:
[1] McKinsey&Company, "The next frontier for digital technologies in oil and gas" 2016