

# Transforming the energy industry with AI





## Preface

“Transforming the energy industry with AI” is an MIT Technology Review Insights report, sponsored by Siemens Energy. The report is based on in-depth interviews with IT and cybersecurity leaders at oil and gas companies worldwide, conducted in September and October 2020. It examines the operational benefits and cybersecurity vulnerabilities that result from the increasing need for companies to digitally transform their businesses, and the measures needed to stay secure and competitive in today’s business climate.

We’d like to thank the following executives and industry observers for their time and insight:

**Khaled Al Blooshi**, Vice President, Digital Products and Innovation,  
Abu Dhabi National Oil Company

**Dr. Reem F. Al Shammari**, Chief Information Security Officer, Kuwait Oil Company

**Filipe Beato**, Project Lead, Centre for Cybersecurity, World Economic Forum

**Edward Chiu**, Cybersecurity Strategist, Chevron

**Phillip Cornell**, Senior Fellow, Atlantic Council Global Energy Center

**Anna Dubovik**, Head of Advanced Analytics and Machine Learning, Gazprom Neft

**Chris Foster**, Vice President, Information Services, and Chief Information Officer, TC Energy

**Javier García Quintela**, Chief Information Security Officer, Repsol

**Angela Haun**, Executive Director, Oil and Natural Gas Information Sharing  
and Analysis Center

**Pedro Jatobá**, Chief Generation Officer, Eletrobras

**Santiago Julian Lopez Galanes**, Chief Information Security Officer, Pampa Energía

**Ken Munro**, Partner, Pen Test Partners

**David Myers**, Chief Information Officer, Technology Infrastructure and Security, Diversified  
Gas & Oil

**Leo Simonovich**, Vice President and Global Head, Industrial Cyber and  
Digital Security, Siemens Energy

**Sridhar Sudarsan**, Chief Technology Officer, SparkCognition

## Foreword

The oil and gas sector has dramatically changed from prior decades. Low prices and market demand for decreased environmental impact make efficiency essential for competitive enterprises. Information technologies (IT) that revolutionized the wider economy have been repurposed and deployed to digitize operating technologies (OT) to produce commercial gains through automation across the industry. On the heels of digitization, a subsequent innovation wave uses artificial intelligence (AI) to further optimize automated systems.

These revolutions in the operating environment occurred rapidly and opened a new set of opportunities and risks that the oil and gas sector must balance – the benefits of digitalization and the need for cybersecurity. With every facet of oil and gas exploration, extraction, refinement, and transportation permeated with digital devices, the monitoring and protection of smart infrastructure is now an essential part of any oil and gas organization's operational responsibilities. The tremendous financial and geopolitical value of oil and gas products and infrastructure make them attractive targets for both criminal organizations and state-backed attackers able to invest significantly in novel attacks. Companies in the oil and gas sector will need to not only maintain current defenses, but continually improve their cyber resilience – both to detect and prevent attacks, and to withstand and recover from those that occur.

Cybersecurity for the oil and gas sector will require bringing together disparate knowledge bases – the innovations flowing from IT and AI researchers, the operation of interlinked oil and gas infrastructure, and the cybersecurity practices appropriate to OT environments that bridge the physical and digital worlds. Oil and gas organizations increasingly recognize that cybersecurity practices cannot be transferred from IT to OT on a one-to-one basis, but must be tailored to the specific needs and constraints of a production environment and its equipment. Detecting and preventing attacks on OT require monitoring system conditions with context and an understanding of how components and conditions interact, and technologies that increasingly adapt AI techniques for efficient and scalable cybersecurity.

This report seeks insight from leading practitioners in the oil and gas sector to provide an understanding of the state of the industry and its future, with reference to specific case studies. Collectively, these insights provide a foundation for future collaboration and partnerships.

One thing is clear: only by working together across these areas of expertise can we hope to secure the digital transformation in the oil and gas sector.

**Leo Simonovich**

*Vice President and Global Head, Industrial Cyber and Digital Security*  
Siemens Energy

# CONTENTS

<b>Preface</b> .....	<b>2</b>
<b>Foreword</b> .....	<b>3</b>
<b>1. Executive summary</b> .....	<b>5</b>
<b>2. Cybersecurity, AI, and digitalization</b> .....	<b>6</b>
Operations optimized by AI .....	6
Interconnectivity and AI.....	7
Protecting OT systems.....	8
<b>3. Cybersecurity and AI at the core</b> .....	<b>10</b>
Adopting AI to stay secure.....	10
AI for increased monitoring of OT systems.....	10
Building a data strategy for AI .....	11
<b>4. Partner to secure and transform</b> .....	<b>12</b>
Partnering for innovation .....	12
Partnering for technology .....	13
Partnering for a collective defense .....	14
<b>5. Conclusion: AI is the here and now for oil and gas companies</b> .....	<b>16</b>
About MIT Technology Review Insights.....	17
From the sponsor .....	17

# 01 Executive summary

For oil and gas companies, digital transformation is a priority – not only as a way to modernize the enterprise, but also to secure the entire energy ecosystem. With that lens, the urgency of applying artificial intelligence and machine-learning capabilities for optimization and cybersecurity becomes clear, especially as threat actors increasingly target connected devices and operating systems, putting the oil and gas industry in collective danger. The year-over-year explosion in industry-specific attacks underscores the need for meaningful advancements and maturity in cybersecurity programs.

However, most companies don't have the resources to implement sophisticated artificial intelligence (AI) programs to stay secure and advance digital capabilities on their own. Irrespective of size, available budget, and in-house personnel, all energy companies must manage operations and security fundamentals to ensure they have visibility and monitoring across powerful digital tools to remain resilient and competitive. The achievement of that goal is much more likely in partnership with the right experts.

MIT Technology Review Insights, in association with Siemens Energy, spoke to more than a dozen information technology (IT) and cybersecurity executives at oil and gas companies worldwide to gain insight about how AI is affecting their digital transformation and cybersecurity strategies in oil and gas operating environments. Here are the key findings:

- **Oil and gas companies are under pressure to adapt to dramatic changes in the global business environment.** The coronavirus pandemic dealt a stunning blow to the global economy in 2020, contributing to an extended trend of lower prices and heightening the value of increased efficiency to compensate for market pressures. Companies are now forced to operate in a business climate that

necessitates remote working, with the added pressure to manage the environmental impact of operations growing ever stronger. These combined factors are pushing oil and gas companies to pivot to new, streamlined ways of working, making digital technology adoption critical.

- **As oil and gas companies digitalize, the risk of cyberattacks increases, as do opportunities for AI.** Companies are adding digital technology for improved productivity, operational efficiency, and security. They're collecting and analyzing data, connecting equipment to the internet of things, and tapping cutting-edge technologies to improve planning and increase profits, as well as to detect and mitigate threats. At the same time, the industry's collective digital transformation is widening the surface for cybercriminals to attack. IT is under threat, as is operational technology – the computing and communications systems that manage and control equipment and industrial operations.
- **Cybersecurity must be at the core of every aspect of companies' digital transformation strategies.** The implementation of new technologies affects interdependent business and operational functions and underlying IT infrastructure. That reality calls for oil and gas companies to shift to a risk management mindset. This includes designing projects and systems within a cybersecurity risk framework that enforces companywide policies and controls. Most important, they now need to access and deploy state-of-the-art cybersecurity tools powered by AI and machine learning to stay ahead of attackers.
- **AI is optimizing and securing energy assets and IT networks for increased monitoring and visibility.** Advancements in digital applications in industrial operating environments are helping improve efficiency and security, detecting machine-speed attacks amidst the complexity of the rapidly digitalizing operating environments.
- **Oil and gas companies look to external partners to guard against growing cyberthreats.** Many companies have insufficient cybersecurity resources to meet their challenges head-on. "We are in a race against the speed of the attackers," Repsol Chief Information Officer Javier Garcia Quintela explains in the report. "We can't provide all the cybersecurity capabilities we need from inside." To move quickly and address their vulnerabilities, companies can find partners that can provide expertise and support as the threat environment expands.

# 02 Cybersecurity, AI, and digitalization

Energy sector organizations are presented with a major opportunity to deploy artificial intelligence (AI) and build out a data strategy that optimizes production and uncovers new business models, as well as secure operational technology. Oil and gas companies are faced with unprecedented uncertainty – depressed oil and gas prices due to the coronavirus pandemic, a multiyear glut in the market, and the drive to go green – and many are making a rapid transition to digitalization as a matter of survival. From moving to the cloud to sharing algorithms, the oil and gas industry is showing there is robust opportunity for organizations to evolve with technological changes.

## Operations optimized by AI

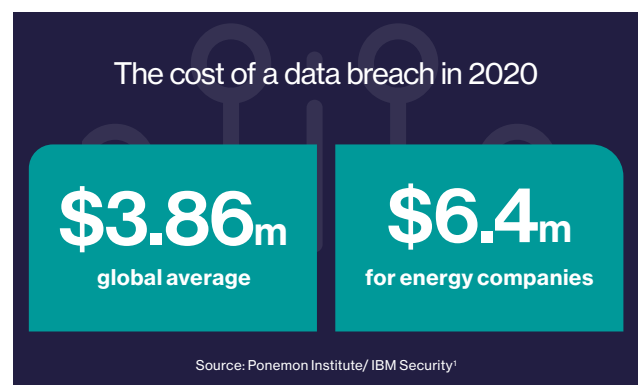
In the oil and gas industry, the digital revolution has enabled companies to connect physical energy assets with hardware control systems and software programs, which improves operational efficiency, reduces costs, and cuts emissions. This trend is due to the convergence of energy assets connected to operational technology (OT) systems, which manage, monitor, and control energy assets and critical infrastructure, and information technology (IT) networks that companies use to optimize data across their corporate environments.

With billions of OT and IT data points captured from physical assets each day, oil and gas companies are now turning to built-for-purpose AI tools to provide visibility and monitoring across their industrial operating environments—both to make technologies and operations more efficient, and for protection against cyberattacks in an expanded threat landscape. Because energy companies' business models rely on the convergence of

OT and IT data, companies see AI as an important tool to gain visibility into their digital ecosystems and understand the context of their operating environments. Enterprises that build cyber-first digital deployments similarly have to accommodate emerging technologies, such as AI and machine learning, but spend less time on strategic realignment or change management.

Importantly, for oil and gas companies, AI, which may have once been reserved for specialized applications, is now optimizing everyday operations and providing critical cybersecurity defense for OT assets. Leo Simonovich, vice president and global head of industrial cyber and digital security at Siemens Energy, argues, “Oil and gas companies are becoming digital companies, and there shouldn't be a trade-off between security and digitalization.” Therefore, Simonovich continues, “security needs to be part of the digital strategy, and security needs to scale with digitalization.”

To navigate today's volatile business landscape, oil and gas companies need to simultaneously identify



## Digital transformation case study series

**For oil and gas titans** with deep pockets, digitalization is recognized as a differentiator and, as such, is a well-funded priority. However, even small and midsize companies can find efficiencies with digitalization.

Discussions with industry executives provide insight into how companies are implementing new technologies.

### AI reduces maintenance costs at ADNOC

Digitalization is contributing to time and cost savings as well as worker safety at Abu Dhabi National Oil Company (ADNOC), according to Khaled Al Blooshi, vice president of digital products. Before digital programs were used in production planning, the cycle was time- and labor-intensive, with hundreds of Excel spreadsheets moving back and forth among business units. "This entire process used to take months to do, and any change in our production plans was near impossible," Al Blooshi says.

ADNOC responded by creating digital twins of all the company's assets and plants. "Today, I have my entire ADNOC value chain on a simulation model," Al Blooshi explains. "I can run what-if scenarios with a couple of clicks to understand, for example, the impact of a refinery being down for maintenance, or introducing a new crude for processing, or initiating kerosene production." With some adjustments to the model over a few hours, "we have our new production plan ready to be dispatched to the operating companies," he says.

ADNOC is aiming to reduce maintenance costs by 20% using AI to improve planning and scheduling by evaluating performance data. "We can extend the life of the asset and, in some cases, we have safely extended the maintenance cycle to tens of thousands of hours for several turbines and pumps, and we are updating our maintenance policies to reflect the same." Al Blooshi says.

optimization opportunities and cybersecurity gaps in their digitalization strategies. That means building AI and cybersecurity into digital deployments from the ground up, not bolting them on afterward.

### Interconnectivity and AI

For companies that work all over the world, centralizing data and managing it to optimize exploration and production activity is an enormous challenge. The need for interconnection has given rise to the industrial internet of things (IIoT), ushering in the fourth industrial revolution, a new era that builds on and extends the impact of digitalization. Communication enabled by connected equipment, enormous amounts of data collection, and disparate devices is leading to faster and better decision-making and greater operational efficiencies. And as that data collection increases, AI and machine learning will be the most efficient and rapid way to interpret and act on it.

### Gazprom Neft identifies exploration horizons with AI

According to Anna Dubovik, head of advanced analytics at Russian oil giant Gazprom Neft, the company began introductory market research on digital technologies in 2017, evaluating offerings and identifying resources. Two years ago, it began aggressively implementing digital tools, focusing on exploration – specifically, seismic analysis. The reason, Dubovik says, is the high cost of a mistake during the first stages of exploration. Error in this step affects every step that follows. Gazprom Neft began using AI algorithms to identify exploration horizons in its seismic data analysis.

"A year ago, AI was treated by geophysicists as a research tool for perspective solutions. But now we are rolling out on actual fields, which are either in development or in exploration, and have seen stunning results." Dubovik continues: "When everything went into lockdown, due to the coronavirus, people became more inclined to use digital transformation tools. This was a perfect opportunity to switch on AI, which doesn't fear viruses and doesn't need vacation or sick leave. It simply does what is required."

However, these same digital advantages leave the oil and gas industry more vulnerable to attacks. Managing the cybersecurity threat to oil and gas operations is complicated by aging infrastructure that is often disconnected or has intermittent connectivity. When companies bolster monitoring capabilities by connecting legacy equipment, they commonly use bolt-on technologies that provide quick functionality but fail to provide adequate cybersecurity. In this way, older assets become part of a broader mesh system already carrying huge volumes of data from more modern equipment. For example, each modern offshore drilling platform is outfitted with approximately 80,000 sensors and generates an estimated 15 petabytes of data during its working life. Solutions need to cover the full breadth of the operations portfolio, ranging from intermittently connected devices and legacy equipment to high-volume, unmanned assets.

Filipe Beato, project lead at the World Economic Forum's Centre for Cybersecurity, cautions that this interconnectivity amplifies cybersecurity challenges and must be top of mind for industry decision-makers. "The

fourth industrial revolution drove growth and innovation in the oil and gas industry, and now more than ever is the time to embed cybersecurity in its business models and strategies," he says.

## Protecting OT systems

Until recently, cyberattacks primarily targeted IT environments, like PCs, workstations, and mobile devices. But the convergence and connectedness of IT and OT

### For Diversified Gas & Oil first cloud, then AI

David Myers, SVP, chief information officer at Diversified Gas & Oil (DGO), says digital transformation is the enabler for his company, which he describes as "a company that looks like and feels like a startup but with existing and extensive operations."

He explains that growth for DGO means acquisition. "We went from approximately 80 employees in late 2016 to 1,100 employees today, and from about 10,000 to 70,000 producing wells, with more than \$2 billion in acquisitions over the last three-and-a-half years." The scale of growth dictates that the company think differently, he says. "Mergers and acquisitions is our key strategy for future growth and that requires fast, efficient, and scalable platforms."

Investing in the right technology matters. Myers explains, "we made the decision to jump 100% to the cloud to support our growth strategy," and that has made all the difference to DGO. Myers continues, "[If we hadn't], I'd be fighting a much bigger battle from an integration speed and flexibility standpoint, as well as our ability to implement cybersecurity controls." For Myers, the cloud allows for efficiency and scale, and supports data warehousing; and data means making better and faster decisions allowing for future deployment of AI for even more scale. His plan: "First, get our data in order and consistent; second, build out business models; and third, use AI to automate and scale."



66%

**of oil and gas company executives say they benefit from digitization even with increased cybersecurity risk.**

Source: Ponemon Institute/Siemens Energy<sup>2</sup>

means that protecting the entire system against cyberattacks is now required. The challenge is to stay ahead of attackers that see this newly connected environment as an opportunity to disrupt physical devices and processes. This type of interference in critical infrastructure could have catastrophic security, economic, and environmental repercussions.

A case in point is a 2017 cyberattack on a SABIC refinery owned by chemical manufacturer Saudi Aramco, which investigators believe was intended to cause an explosion. The attack was unsuccessful, but it's indicative of a cybersecurity landscape that includes aggressive nation-state actors openly targeting one another by going after critical infrastructure. Oil and gas companies are tackling these fluid safety challenges as they adopt new ways of working, including remote operations. They're gathering and analyzing more data to identify risks and develop safer protocols as work environments change, but a greater reliance on OT data makes protecting IT more important than ever. While improved communication enhances the ability to manage assets and resources, it also broadens the interface between IT and OT, creating a dramatically larger attack surface for potential hackers.

As Ken Munro, a security expert at Pen Test Partners, explains, "People within the IT side of the business want management data to improve efficiencies," but in the

process of gaining access to OT systems, "network segregation has started to break down."

Even cyberattacks that are less severe than the SABIC incident can still cause significant damage—compromising data and devices, interrupting operations, and resulting in extensive downtime and lost revenue. They also can damage the reputations of targeted companies that lose trust with customers dependent on integrity of supply.

With more than 38 billion devices expected to be connected to the internet of things this year, the threat horizon continues to expand, according to IBM Security's X-Force Threat Intelligence Index 2020.<sup>3</sup> The breakdown of system segregation is opening the door to cyberattacks on industrial control systems and similar OT assets, with attacks increasing more than 2,000% from 2018 to 2019. The energy sector is the ninth-most targeted industry in the X-Force ranking.

"In essence, digitalization and cybersecurity are two sides of the same coin," says Simonovich. That's because advances in digitalization drive the need for greater cybersecurity.

And that's the pinch point for oil and gas companies that require industrial cybersecurity solutions – securing massive physical operations, as well as the underlying software, requires a holistic view on the entire ecosystem.

## Pampa Energía promotes security by design

Pampa Energía has been leading the digitalization charge in Argentina. According to Chief Information Security Officer Santiago Julian Lopez Galanes, in 2019 the company completed a cybersecurity-maturity assessment of its critical infrastructure and began executing a multiyear action plan that, according to Lopez, is on par with world-class best practices in the industry.

Current digitalization efforts are directed toward optimizing performance and condition-based maintenance, including the implementation of an online monitoring program that links operations,

maintenance, and plant experts, with the support of AI and machine-learning software. Lopez notes, "We have to facilitate and promote security by design, which will enable the secure digital transformation of the company."

For example, in 2020, the company rolled out a service for monitoring cybersecurity events to ensure "security incidents in OT environments were correctly identified, analyzed, defended, investigated, and reported." All of this data is rolled into an automated dashboard used by stakeholders to make decisions.

# 03 Cybersecurity and AI at the core

The move to digital transformation is complex, especially when integrating new technologies, like AI, which affect a number of business and IT functions. The move to a more digitalized workplace has changed the way projects are executed, shifting the focus from a compliance-based decision-making framework to a risk management mindset.

## Adopting AI to stay secure

For oil and gas companies, getting ahead of cyberthreats means gaining visibility into operations to understand vulnerabilities and implementing technologies that provide depth and scalability. A strong defense must take advantage of AI and machine learning to establish future-proof protections that can accommodate changes in the cyberthreat landscape.

However, the industry has some way to go to reach this goal. In a 2018 report, only 36% of oil and gas companies had invested in big data and analytics, and a meager 13% used the insights gained from technology to enhance business intelligence. Companies have not embedded big data and analytics completely in their systems, which means they aren't getting full value from the technology.<sup>4</sup> Increasingly, the application of AI to industrial security is on their agenda.

## AI for increased monitoring of OT systems

Petrobras, the national oil company in Brazil, established its digital transformation program several years ago but has seen enormous progress this year as a direct result of the covid-19 pandemic, which the company says accelerated digitalization and allowed it to accomplish more in six months than it expected to achieve over six years.

Petrobras previously instituted an office for digital transformation made of three components to align its digital journey with the company's strategic pillars. The first applies innovative technologies such as scalable infrastructure expansion and cloud-first application development, implementation of modern architecture, and integration of company data. The second promotes the adoption of a culture of digital innovation and includes a number of training and research facilities. The third component focuses on redesigning processes to accommodate digital transformation.

As the rate of digitalization accelerated in 2020 with the adoption of cloud computing, AI, and an expanding internet of things, Petrobras focused on evolving its IT security and applied AI to improve monitoring of critical OT systems. In fact, the company uses AI and machine-learning techniques in a range of business processes to improve efficiencies.

### Building a data strategy for AI

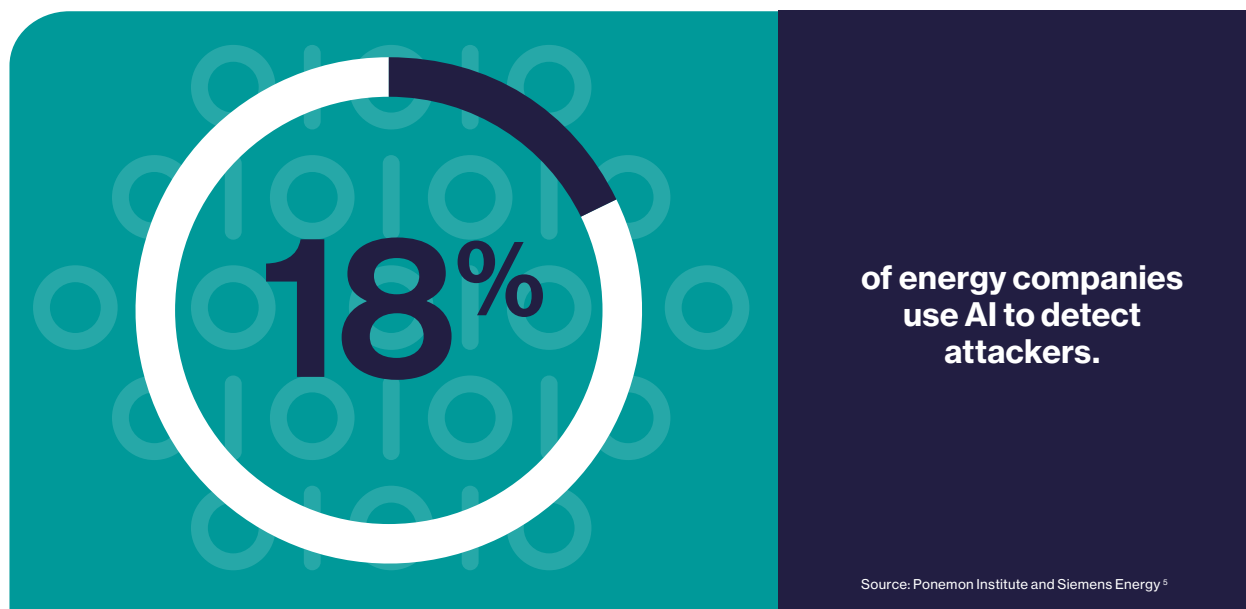
Spain's Repsol began talking internally about digitalizing operations in 2017 and allocated resources to develop a digital transformation plan that has delivered tangible results. According to CISO Javier García Quintela, the plan facilitated cultural changes that affect every part of the company: "how we design our projects, how we build our systems, the methodologies that we use, the types of technologies, and the strategic vendors we use, and even how we deliver IT, interact with customers, and make decisions."

A little more than a year ago, Repsol designed the necessary cybersecurity practices to protect its OT environments. The high level of automation in its industrial systems led Repsol to take a hard look at cybersecurity for the OT side of its business as well, and to put in place a framework for cybersecurity. "Safety is the top priority," García says, "Current practice introduces not only

technology but also roles, ways of working, allocation of responsibilities, controls, and policies so cybersecurity practices can be managed in a holistic way."

Real-time data harvesting and management is foundational to Repsol's plans, and the company is turning to monitoring to measure and improve productivity, track performance, adjust for inefficiencies, schedule maintenance work, and make better, faster decisions, García says. "That's the main focus of our digital program." Looking to the future, Repsol is introducing AI to analyze and correlate information. "When you manage a very high volume of information on a recurrent basis, you need to take advantage of AI to understand what is happening. The most interesting technology for achieving that level of understanding in the next years is going to be AI," he says.

New cybersecurity advancements continue to change the cost-benefit proposition for the energy sector. Machine-learning tools trained to recognize normal operations can identify anomalies and flag potential problems, and AI algorithms analyze performance data to initiate corrective actions and streamline processes. Because these technologies improve as they are implemented, they are even more impactful over time.



## Partner to secure and transformation

An important consideration is how to partner with experienced resources, whether that's with a specialized startup or a joint venture to form a novel way of working. For example, original equipment manufacturers can not only secure their own products but increase security throughout the entire ecosystem for both OT and IT operations, which can help many enterprises. For small and medium-sized energy companies, getting this access to cutting-edge AI, as well as industry-standard monitoring, detection, and cyberattack prevention capabilities, is a game-changer. Having a cybersecurity

risk strategy available for these smaller companies means the entire energy system is more secure.

### Partnering for innovation

Real innovation for oil-and-gas-specific cybersecurity is happening, and partnerships between original equipment manufacturers and tech vendors are bringing it into the mainstream, says Siemens Energy's Simonovich. He points to the joint effort by Siemens Energy and AI startup SparkCognition to protect entire fleets of assets such as pipelines or power generators. The result of their work is DeepArmor Industrial, which uses AI to flag

### Gazprom Neft encourages collaboration with AI

Gazprom Neft's Anna Dubovik says AI is dramatically changing how the company identifies drilling horizons, or potential targets. "The speed and accuracy are incredible," she says. In five days, one expert with expensive proprietary software identified drilling in 50% of the surveyed area with 25% traceability; however, AI found horizons in 95% of the area with 100% traceability, which tells the company exactly where to drill.

Not only is Gazprom Neft improving its own accuracy, the company is sharing what it has accomplished with the industry, posting its technology on the GitHub development platform. "Everybody who is trying to adopt data science

in the industry can just take our libraries and the data they have inside and adapt them to make the digital transformation and AI applications faster in their company," she explains. This move also encourages collaboration. "We are hoping the tools are improved through open sourcing. Everyone who wants to contribute can contribute to it."

Dubovik is optimistic about the potential results: "Companies in oil and gas are super closed, and very few have entered this niche of open source and collaborating. Based on the examples that we see in high tech, however, this is definitely the direction to go."

cyberthreats targeting end-point energy assets before they execute, and home in on never-seen-before “zero-day” cyberattacks. The system can ferret out such exploits, says SparkCognition CTO Sridhar Sudarsan, because machine-learning algorithms “find why something becomes malware, and that’s what we go and defend against.”

The product can protect systems in any industry, but it’s particularly tailored to address scenarios common in oil and gas infrastructure – for example, it can work autonomously on older assets that aren’t connected to a network – by providing protection on the edge customized to client workflows. That precision defense is owed to the unique chemistry of the partnership, says Sudarsan – namely, Siemens Energy’s long history of protecting oil and gas facilities and SparkCognition’s native AI know-how.

“If we do this by ourselves, we don’t have the experience of every single asset and environment, and if Siemens Energy tries to do this on their own, they don’t have the software and the AI experience and the expertise that we have.” Sudarsan continues, “By coming together, we were able to innovate and scale to solve a largely unaddressed space.”

### Partnering for technology

Alongside the collaborative work among tech companies to bring together AI and cybersecurity is another kind of partnership: that between vendors and oil and gas companies themselves. As they adopt new technologies, improve operations, and streamline activity, many are also looking for opportunities to outsource essential cybersecurity operations. Some of this is driven by shrinking budgets.

A recent report by global energy consultancy Wood Mackenzie examined the effects of the market on oil and gas companies.<sup>6</sup> Analyst Preston Cody believes current conditions are forcing change. “Before the 2020 crisis, the dominant attitude in the industry was to build analytics capabilities in-house,” he writes. The approach wasn’t terribly effective. The reason is, “true expertise in data management and analytics is outside traditional upstream core competencies.” He contends that as low oil prices persist, companies will be more inclined to add to their digital toolboxes by buying, not building, technology, and finding ways to collaborate.

**“Strategic partnerships provide access to more experts that we can work with and build on each other’s strengths to enhance our security”**

– Chris Foster, Vice President of Information Services and CIO, TC Energy

### AI and cybersecurity work together at Chevron

Chevron has been on its digital journey for several years now and cybersecurity strategist Edward Chiu believes his company has made considerable progress. “We are still pretty early in our AI journey,” he says, “but we are putting a lot of emphasis on AI, machine learning, business analysis, and streamlining business workflows. Any AI technique we can use to improve our business’ bottom line, we’re exploring – on petrotechnical and other IT applications, including cyberdefense and analytics,” he says.

Chiu and his team evaluate new technologies and the potential for applying them at Chevron. “We try to divide the emerging technologies into different horizons,” he says, explaining that a “horizon” indicates the level of maturity of a technology and when it’s likely to be implemented. “In terms of cybersecurity, we identify the security impact of emerging technologies in different horizons, and we always look at deployment potential.”

For some companies, this approach is new. Others saw the value in finding strong technology partners earlier on. Saudi Aramco took a big step toward broader partnering in 2017, when it signed a memorandum of understanding with tech company Honeywell to increase throughput and production and improve the reliability of its operations by using Honeywell's cloud-based and predictive analytics services. In a statement, the company said the agreement "supports the development and diversification of Saudi Arabia's oil and gas sector and accelerates the benefits of the IIoT within Saudi Aramco's operations." According to Saudi Aramco president and CEO Amin H. Nasser, the decision to partner with technology leaders adds strategic value to the company, the sector, and the "country as a whole."<sup>7</sup>

Other companies looking to cloud services like Amazon Web Services for innovation rely on them for cybersecurity as well. "It doesn't mean that they pawn off the responsibility for information security to Amazon," the Atlantic Council's Cornell says, "but those services are definitely secure enough as long as they are managed right."

For Chris Foster, vice president of information services and chief information officer at North American pipeline company TC Energy, the exciting part is not being in the cloud, which he says is "just someone else's computer."

The transformational piece is the access to otherwise prohibitively costly tools.

"One of the challenges in cyberspace is that things are moving so fast," Foster says. "The volume of connected devices is growing exponentially," and this makes keeping up with security extremely difficult, particularly in a sector that uses infrastructure designed 30 or 40 years ago.

As he sees it, the smartest way to improve cybersecurity quickly is to expand the cybersecurity team with experienced partners. "Although we've got some smart and experienced people that understand and are committed to advancing our cybersecurity posture and program, strategic partnerships provide access to more experts that we can work with and build on each other's strengths to enhance our security," Foster says. "AWS might be the biggest cybersecurity company you've never heard of – because that's not how they advertise themselves – but they're absolutely one of our partners now."

### Partnering for a collective defense

For many companies, partnering is a way to advance cybersecurity rapidly enough to move past the threats presented by today's hackers. Repsol, for example, works with a range of partners to add expertise to its in-house team.

## ADNOC partners for AI innovation

ADNOC began its digitalization journey early, implementing from the outset programs that Khaled Al Blooshi, vice president for digital products, describes as "transformational." The company moved swiftly to employ technologies to create efficiencies and improve project planning and execution and has been at the forefront of adoption.

In October 2020, ADNOC took its technology program to a new level with the formation of an AI joint venture company with Abu Dhabi-based cloud computing company Group 42.

The joint venture, called AIQ, will develop and commercialize AI products and applications

specifically for the oil and gas industry. According to Sultan Al Jaber, the United Arab Emirates' minister of industry and advanced technology and ADNOC Group CEO, the goal is "to accelerate the development of new AI solutions to optimize processes, improve planning, and increase profitability for ADNOC and the wider oil and gas industry."<sup>8</sup>

The formation of AIQ follows other ADNOC transformation initiatives that include the AI and big data-driven Panorama Digital Command Center, big data modeling tools for value chain optimization, computer-vision technologies, predictive maintenance machine-learning technologies, and blockchain for hydrocarbon accounting.

“We are in a race against the speed of the attackers,” CISO García explains. “We can’t provide all the cybersecurity capabilities we need from inside. We work with different companies for different types of services, and all those companies bring valuable knowledge.”


Pedro Jatobá, chief generation officer at Eletrobras, the national power generation transmission company in Brazil, says partnering is allowing the company to modernize its infrastructure, which includes 71,000 km of long-distance transmission lines, some constructed in the 1960s. To make the kind of rapid progress necessary, the company needs to work with outside experts, Jatobá says. And it is doing so with the cooperation and significant contribution from universities and industrial players like SparkCognition and Siemens Energy, as well as a continued partnership with SAP.

Kuwait Oil Company’s CISO Dr. Reem F. Al Shammary sees advantages in collaborating for stronger cyber defenses in what she refers to as “a trusted circle of sharing threat intelligence.” This approach makes defending against cyberattacks more effective and resilient, she says. “We are stronger together. When we trust each other and communicate, when we share strategies and best practices, when we collaborate in this rapidly changing industry, our collaboration will be crucial and productive, empowering us and giving us a better cybersecurity posture for our operations against the ever increasing threat landscape.”

There’s also more help out there today, says Cornell. Industry groups are better equipped to help smaller companies that are trying to design and implement an effective cybersecurity strategy. “There are resources out there more than there ever have been in the past.”

One organization focused on collaborating across the industry is the nonprofit Oil and Natural Gas Information Sharing and Analysis Center. Its mission is to serve as a central point of coordination for the industry and foster trust among industry member companies, partner organizations, and government agencies. The organization facilitates communication, allowing companies to share and analyze timely cyberthreat information to help protect exploration and production, transportation, refining, and delivery systems.

“The importance of collaboration cannot be emphasized enough,” says Angela Haun, executive director. “Building



“Collaboration gives us a better cybersecurity posture for our operations against the ever increasing threat landscape.”

—Dr. Reem F. Al Shammary, Chief Information Security Officer, Kuwait Oil Company

relationships and developing trust is fundamental to effective collaboration.” Without the ability to discuss cyber issues in a safe place, oil and gas companies are at an enormous disadvantage.

Beato of the World Economic Forum agrees. The risk of oil and gas operations being hacked or compromised is real, and most companies do not have the resources to tackle this problem alone given the complexity of oil and gas supply chains. “Only through public-private collaboration with all stakeholders will we achieve effective cyber resilience across the industry.”

# 05 Conclusion: AI is the here and now for oil and gas companies

Oil and gas companies jolted into remote work and accelerated digital transformation will continue on that path. Those companies already on their digital journey are poised to leap ahead with AI. The mantra many take up will be “spend money to make money”—but the winners will take advantage of digitization by also adopting modern cybersecurity efforts now with a more aggressive move to the cloud and beyond.

- **As vaccines roll out, the global economy will come back, too.** But even as oil prices inevitably rise, the oil and gas industry will continue to consolidate and modernize to glean efficiencies and save on costs in the energy transition.
- **Adopting and scaling AI will increase.** There will be a growing need for companies to further automation, machine learning, and AI capabilities to not just compete but make the best use of the immense amount of data now captured because of digital transformation efforts.
- **Cybersecurity needs AI to complete cyberdefense.** The fight to avoid and contain ever-more sophisticated cybersecurity attacks will necessitate focused cybersecurity and AI efforts.
- **Small and midsize companies will benefit from partnerships.** There is no “go-it-alone” strategy. Partnering will help companies fulfill the expertise gap and ultimately stay secure — especially these small and midsize oil and gas enterprises that are an integral, but vulnerable, part of the ecosystem.

Laurel Ruma and Jason Sparapani edited the report, and Nicola Crepaldi was the publisher. The views expressed within are those of MIT Technology Review Insights, which is editorially independent.

## About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of MIT Technology Review, the world's longest-running technology magazine, backed by the world's foremost technology institution – producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. And through its growing MIT Technology Review Global Panel, Insights has unparalleled access to senior-level executives, innovators, and thought leaders worldwide for surveys and in-depth interviews.

## From the sponsor

Siemens Energy is a global industrial powerhouse operating across the entire energy ecosystem. Focused on the areas of electrification and digitalization, we draw on a 170-year heritage as a producer of mechanical, electrical, and control systems to deliver innovative cybersecurity solutions for the industrial operating environment. We bring over 30 years of unique security insights and expertise to protecting the world's critical infrastructure. Siemens helps energy companies harness the power of digitalization and place cybersecurity at the center of their business models. We leverage artificial intelligence, deep domain expertise, and global reach to help energy companies of all sizes monitor, detect, and prevent attacks before they occur. Our cybersecurity solutions are designed to secure the complete operating environment, from the wellhead to the power meter, working seamlessly across digitally native and legacy assets. Siemens Energy works hand-in-hand with customers and partners to build digital trust, collective defenses, and resiliency toward an efficient, clean, and secure energy future.



### References

1. "Cost of a Data Breach Report 2020," Ponemon Institute and IBM Security.
2. "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?," Ponemon Institute and Siemens Energy, 2019.
3. "X-Force Threat Intelligence Index 2020," IBM X-Force Incident Response and Intelligence Services, February 2020.
4. "Global Big Data in Oil and Gas Exploration and Production Market - Analysis of Growth, Trends and Forecasts (2018-2023)," Market Reports World, February 8, 2018.
5. "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?," Ponemon Institute and Siemens Energy, 2019.
6. "Have budget cuts stalled digitalisation initiatives?" Wood Mackenzie, August 2020.
7. "Honeywell And Saudi Aramco Advance Digitization Of Oil And Gas Industry With New Agreement," (press release) Honeywell, May 23, 2017.
8. "ADNOC and Abu Dhabi-Based Group 42 Launch AIQ – an Artificial Intelligence Joint Venture Company," (press release) Abu Dhabi National Oil Company, October 2020.


### Illustrations

Illustrations assembled by Scott Shultz Design. Cover: Oil refinery, Davooda; Shield icon, VectorCookies, Shutterstock. Internal page elements by Anton Shaparenko, Cube29, Nanmulti, CkyBe, Turbodesign, Shutterstock.


*While every effort has been taken to verify the accuracy of this information, MIT Technology Review Insights cannot accept any responsibility or liability for reliance on any person in this report or any of the information, opinions, or conclusions set out in this report.*



## MIT Technology Review Insights

 [www.technologyreview.com](http://www.technologyreview.com)

 @techreview @mit\_insights

 [insights@technologyreview.com](mailto:insights@technologyreview.com)