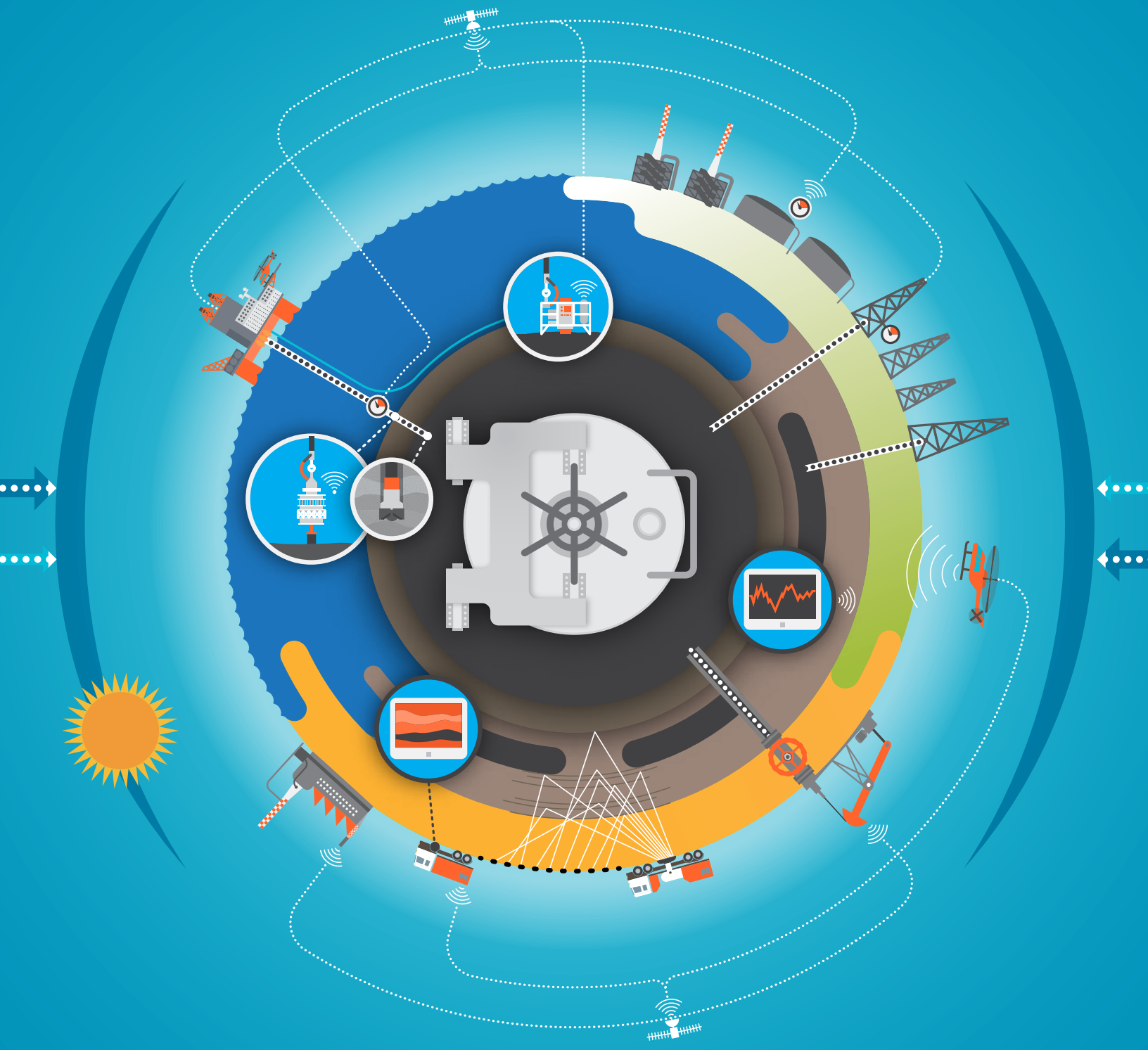
Deloitte.
University Press



Protecting the connected barrels

Cybersecurity for upstream oil and gas

A report by Deloitte Center for Energy Solutions

The Deloitte Center for Energy Solutions provides a forum for innovation, thought leadership, groundbreaking research, and industry collaboration to help companies solve the most complex energy challenges. Through the Center, Deloitte's Energy & Resources group leads the debate on critical topics on the minds of executives—from the impact of legislative and regulatory policy, to operational efficiency, to sustainable and profitable growth. We provide comprehensive solutions through a global network of specialists and thought leaders.

With locations in Houston and Washington, DC, the Center offers interaction through seminars, roundtables, and other forms of engagement where established and growing companies can come together to learn, discuss, and debate.

For more information, visit us at www.deloitte.com/us/energysolutions and @Deloitte4Energy.

COVER IMAGE AND INTERIOR ILLUSTRATION BY INFOMEN

CONTENTS

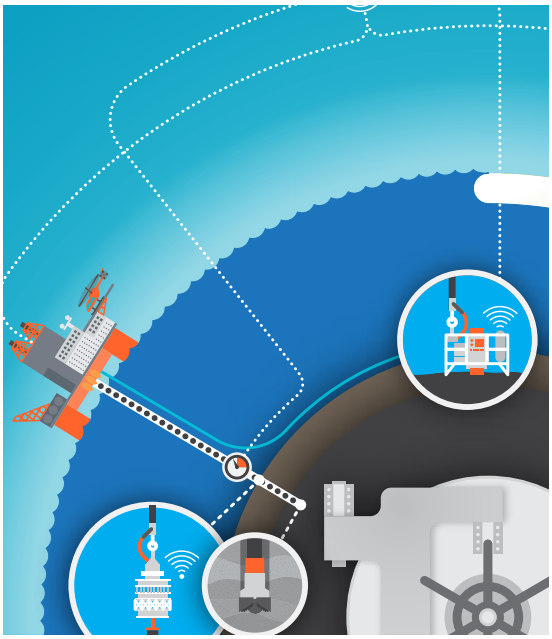
Introduction

Risks—and stakes—keep rising

FOR years, cyber attackers have targeted crude oil and natural gas (O&G) companies, with attacks growing in frequency, sophistication, and impact as the industry employs ever more connected technology. But the industry's cyber maturity is relatively low, and O&G boards show generally limited strategic appreciation of cyber issues.[1]

Why is this so? Perhaps because the industry—engaged in exploration, development, and production of crude oil and natural gas—may simply feel like an unlikely target for cyber-attacks. The business is about barrels, not bytes. In addition, the industry's remote operations and complex data structure provide a natural defense. But with motives of hackers fast evolving—from cyberterrorism to industry espionage to disrupting operations to stealing field data—and companies increasingly basing daily operations on connected technology, risks are rising fast, along with the stakes.

Different areas of the O&G business, naturally, carry different levels of risk and demand different strategies.[2] Our previous article, *An integrated approach to combat cyber risk: Securing industrial operations in oil and gas*, looked at cyber risks and the governance process at an overall O&G industry level; this follow-up explores the upstream value chain of the O&G industry (exploration, development, and production) to assess each operation's cyber vulnerability and outline risk mitigation strategies.



Among the upstream operations, development drilling and production have the highest cyber risk profiles; while seismic imaging has a relatively lower risk profile, the growing business need to digitize, e-store, and feed seismic data into other disciplines could raise its risk profile in the future. A holistic risk management program that is secure, vigilant, and resilient could not only mitigate cyber risks for the most vulnerable operations but also enable all three of an upstream company's operational imperatives: safety of people, reliability of operations, and creation of new value.

Shrugging off cyber threats

In 2016, energy was the industry second most prone to cyber-attacks, with nearly three-quarters of US O&G companies experiencing at least one cyber incident.[3] But in their latest annual filings, only a handful of energy companies cite cyber breaches as a major risk. In fact, many US O&G companies lump cyber risk with other risks such as civil unrest, labor disputes, and weather disruptions; many non-US O&G companies don't mention "cyber" even once in their 100+-page filings.[4]

Worryingly, more and more cyber-attacks are happening on industrial control systems (ICS) of O&G companies in the upstream business, putting at risk worker safety, reputation, and operations as well as the environment. Whether hackers use spyware targeting bidding data of fields, malware infecting production control systems, or denial of service that blocks the flow of information through control systems, they are becoming increasingly sophisticated and, specifically alarming, launching coordinated attacks on the industry. In 2014, for example, hackers launched an all-out assault on 50 O&G companies in Europe using well-researched phishing campaigns and advanced versions of Trojan horse attacks.[5]

It's no surprise that pinpointing the attackers is tough. What complicates defense efforts is that their motives are often equally obscure. According to the Industrial Control Systems Cyber Emergency Response Team, more than a third of the 2015 attacks on critical infrastructure were untraceable or had an unknown "infection vector."[6] That's why cyber breaches remain undetected for days, and why attacks such as Shamoon—the disk-wiping malware that crippled 30,000 computers at Middle Eastern O&G companies in 2012—continue to reappear in one form or another.[7]

True, some estimates put the average energy company's annualized cost of cybercrime at only around $15 million.[8] But a major incident could easily incur costs running into hundreds of millions of dollars and, more importantly, risk people's lives and the nearby environment. If a cyber attacker were to manipulate the cement slurry data coming out of an offshore development well, black out monitors' live views of offshore drilling, or delay the well-flow data required for blowout preventers to stop the eruption of fluids, the impact could be devastating.

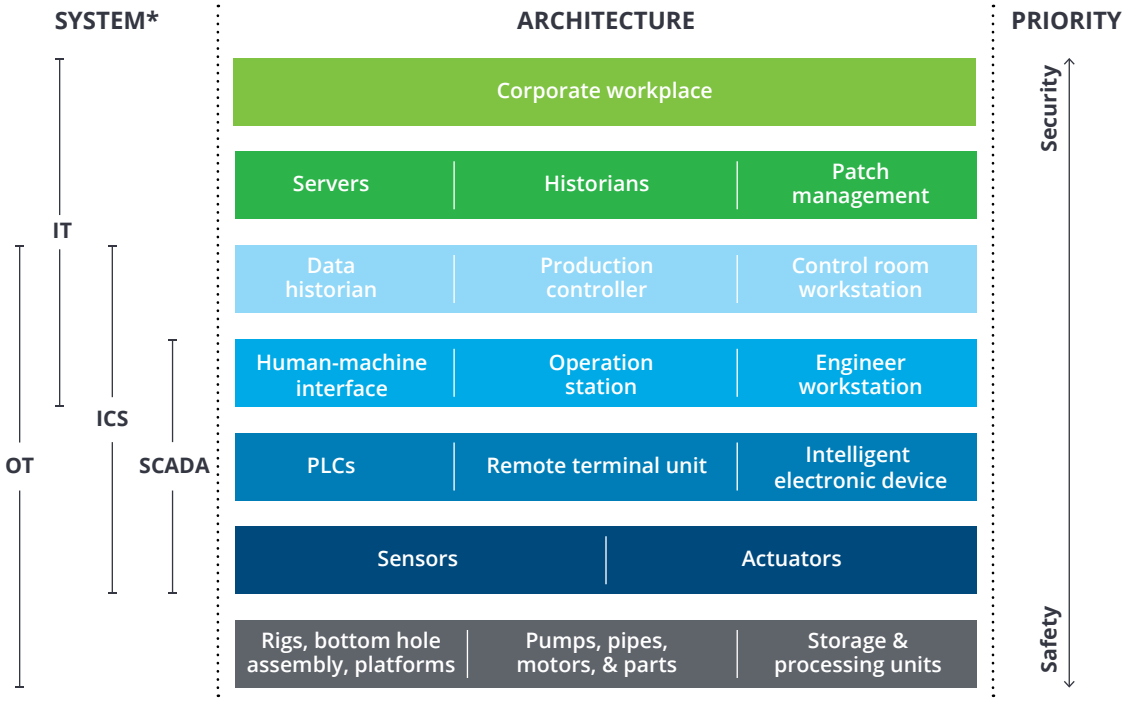
Digitization magnifies the challenges

Apart from the upstream industry's "critical infrastructure" status, a complex ecosystem of computation, networking, and physical operational processes spread around the world makes the industry highly vulnerable to cyber-attacks; in other words, the industry has a large attack surface and many attack vectors[i] (see figure 1). A large O&G company, for instance: uses half a million processors just for oil and gas reservoir simulation; generates, transmits, and stores petabytes of sensitive and competitive field data; and operates and shares thousands of drilling and production control systems spread across geographies, fields, vendors, service providers, and partners.[9]

What adds to this vulnerability is contrasting priorities of companies' operation technology and information technology departments. Operation systems close to drilling and well site operations such as sen-

[i] An attack surface is the total sum of the vulnerabilities in a given computing device or network that are accessible to a hacker. An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome.

Figure 1. Typical IT/OT architecture and cyber concerns of an O&G company



CYBER CONCERNS

- **Complex ecosystem**: Joint operations take place across regions and employ multiple vendors with different security guidelines.
- **Fragmented ownership**: IT and OT were developed with distinct missions, thus cyber ownership and responsibility are fragmented across the organization.
- **Latency concern**: Firewalls could introduce unacceptable latency into time-critical ICS systems that face operational constraints.
- **Inconsistent cyber standards**: A mix of proprietary and off-the-shelf technologies complicates the problem.
- **Irregular patching**: Security patching of many systems is irregular and vendor specific as these systems are in remote, unmanned areas.
- **Legacy concerns**: Many systems have long life cycles (10+ years) that were not built for cybersecurity. Retrofitting or upgrading is costly and impacts operations.

**Acronyms: ICS: Industrial control systems; SCADA: Supervisory control and data acquisition*

Source: Deloitte analysis.

sors and programmable logic controllers are intended to perform tasks with 24X7 availability as their primary attribute, followed by integrity and confidentiality. In contrast, IT systems such as enterprise resource planning have a reverse priority order of confidentiality, integrity, and availability. This clash of objectives—safety versus security—plays out in drilling and production control rooms where engineers fear that stringent IT security measures could introduce unacceptable latency into time-critical control systems, impacting decision making and operational response.

The technical set-up of ICS also carries inherent security challenges. Decisions about ICS software are often made not centrally by corporate IT but, rather, at the field or unit level, resulting in products from different solution providers, based on different technologies, and with different IT security standards. The decade-plus life cycle of wells and ICS systems and ongoing asset sales and purchases add to the diversity problem, making it challenging to account, standardize, upgrade, and retrofit these systems frequently. About 1,350 oil and gas fields globally, for instance, have been producing for more

than 25 years, using systems and equipment from different vintages throughout that period.[10]

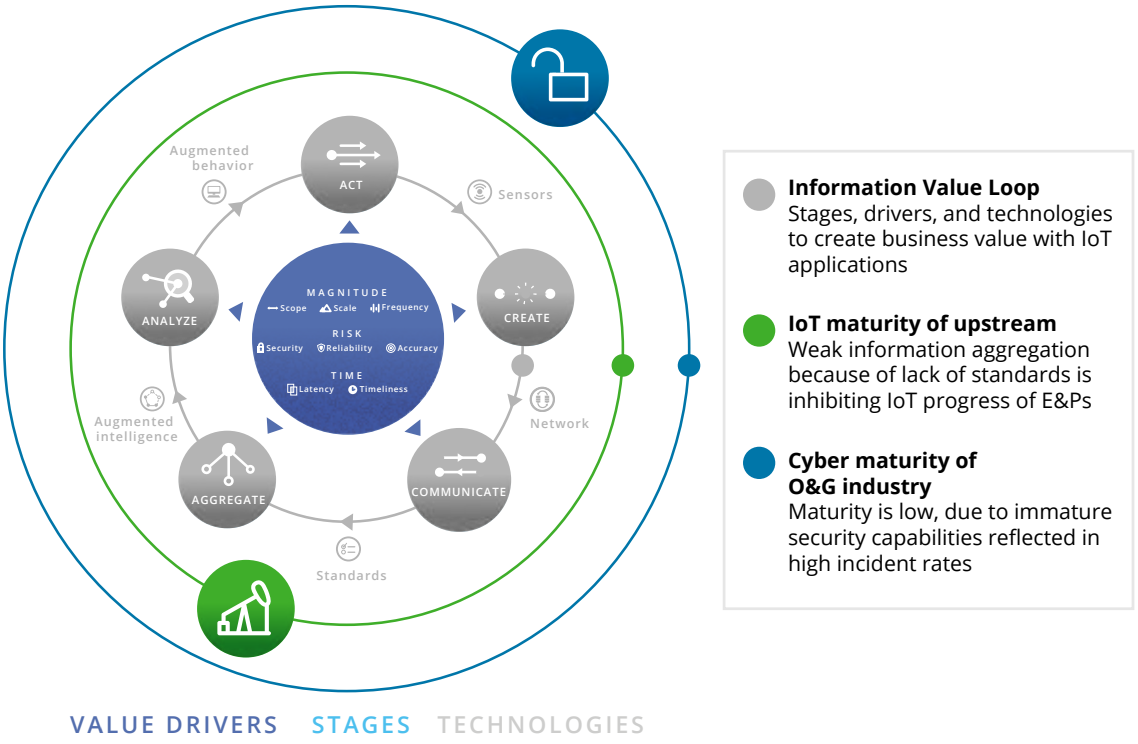
Growing digitization and interconnectedness of operations have heightened cyber risks further. Connected technology, in the embryonic form of digital oil fields or smart fields, has opened up an altogether new landscape of attack vectors for hackers by connecting upstream operations in real time. For example, Shell recently designed a well and controlled the speed and pressure of the drilling in Vaca Muerta, Argentina, from a remote operating center in Canada.[11]

What makes Internet of Things (IoT) technology so powerful but also vulnerable is its ability to create, communicate, aggregate, analyze, and act upon the data—the stages of Deloitte's Information Value Loop (see figure 2). These stages are enabled through sensor technology and, typically, wireless communications networks and several analytical and automated tools, and each is highly vulnerable to security breaches in legacy ICS systems and complex upstream ecosystems. The upstream O&G industry has a dual cyber challenge of safeguarding already-created value and staying ahead of future IoT deployment.

Further, intelligent instrumentation at a field level—devices that can self-process, analyze, and act upon collected data closer to operations rather than at a centralized storage and processing center—have taken cyber risks into the front line of upstream operations. For example, a malicious hacker could slow down the oil extraction process by varying the motor speed and thermal capacity of an integrated sucker rod pump (the "front line" of the oil production process) by altering speed commands sent from internal optimization controllers.

With connected technology's adoption and penetration getting ahead of current cybersecurity practices, it is not just the new IoT-generated *information* and *value* that is at risk. The future opportunity cost—including the safety of personnel and impact on the environment—is at stake.

Figure 2. IoT and cyber maturity of the upstream O&G industry



Source: Deloitte analysis.

Where to begin

Assess vulnerability to prioritize cyber investments

HOW to begin ranking vulnerabilities and priorities, especially when IT and ICS technicalities often cloud strategic appreciation and sponsorship of the cyber issue? For engaging C-suite upstream strategists, it is necessary that the cyber issue be framed in the language of business risks, impacts, and solutions explained at the level of a business unit (offshore, lower 48, international, etc.) or value chain (geophysical surveys to well abandonment). While acknowledging that business units differ from company to company, this paper outlines a detailed cyber vulnerability and severity assessment framework at an aggregate industry value-chain level.

Vulnerability of an upstream operation would be a function of the attack surface (for example, the number of vendors, users, and interfaces or the number and type of industrial control systems and operations); mode and flow of data (physical or digital and unidirectional, bidirectional, or multidirectional); and the existing state of security and controls in place. Severity, on the other hand, includes both direct and in-direct costs in the form of health, environment, and safety incidents, business disruption, legal and regulatory issues, reputational damage, and intellectual property theft (see appendix, explaining our research methodology).

Upstream stages (exploration, development, and production and abandonment) have a distinct cyber vulnerability and severity profile (see figure 3). In fact, within a stage such as development, field development planning has a different cyber risk profile than development drilling. Although each operation needs to be secured, prioritizing security for the most critical, risk-prone operations is essential for determining where to take action first and narrowing the remediation scope. Below, we discuss major critical and risk-prone operations in each stage.

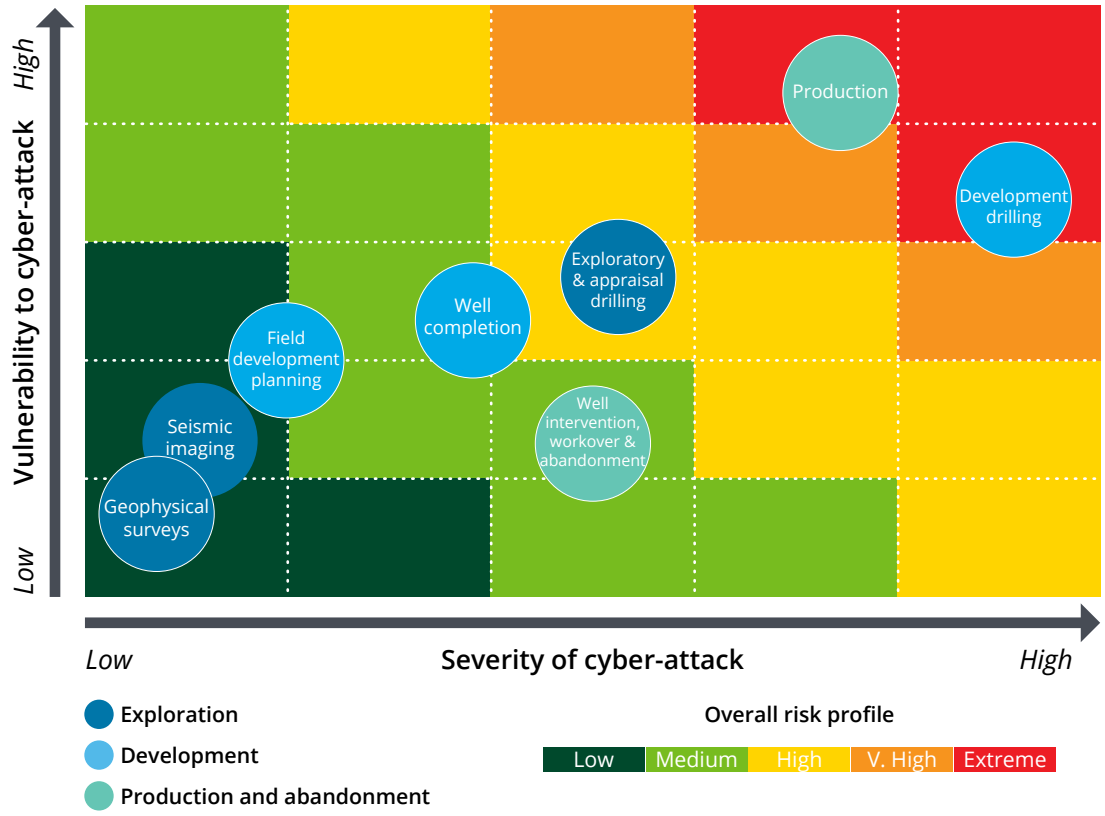
1. Exploration

Of the three major stages, exploration has the lowest cyber vulnerability and severity profile. Its cyber vulnerability is low because the first two operations—seismic imaging and geological and geophysical surveys—have a closed data acquisition system (rock formation data captured through magnetics, geophones, and hydrophones is largely sent via physical tapes and/or processed in proprietary models, which have limited connectedness with the outer world) and a fairly simple ecosystem of vendors (the top three geophysical vendors control 50 to 60 percent of the market and provide a complete suite of offerings).[12] The third operation, exploratory and appraisal drilling, has a higher risk profile but includes many elements of the development stage, covered in the next section.

The likely financial impact of a cyber-attack on geological and geophysical and seismic imaging is low, as upsetting this operation would have a low probability of causing a business disruption or health, environment, and safety risk. However, a company's competitive field data is at most risk in this operation, and an attack might long remain unnoticed due to no direct costs or visible impacts. For instance, the hackers behind the 2011 Night Dragon cyber-attack disabled proxy settings and, for years, used remote administrative tools to steal field exploration and bidding data of many O&G companies.[13]

Although the current exploration workflow has a relatively safe cyber risk profile, companies are increasingly using advanced gravity wave sensors to improve accuracy of subsurface imaging and putting more and more terabytes of seismic data to use by

Figure 3. Cyber vulnerability/severity matrix by upstream operations



Note: Refer to the appendix for further details.

Source: Deloitte analysis.

digitizing, storing, and processing it on supercomputers. CNOOC, for example, reduced its seismic data computing time from two months to just a few days and increased its storage performance by 4.4 times by deploying open-source, high-volume servers scalable to multiple storage clusters.[14]

Expanding such software-based, high-performance computing and storage advancements would, no doubt, exponentially enable IoT-based value creation. But when this exploration data starts feeding in real time into cross-discipline upstream operations such as drilling plans of nearby fields, completion designs, and reserve estimations, a cyber-attack's impact would multiply, from a potential revenue loss to a significant business disruption.[15]

2. Development

Within the O&G value chain, development of oil and gas wells is an operation particularly exposed to cyber incidents. The development drilling operation involves similar techniques to those used in exploratory and appraisal drilling but has a much bigger cyber-attack vector, due to higher drilling activity, expansive infrastructure and services both above and below the surface, and a complex ecosystem of engineering firms, equipment and material suppliers, drillers and service firms, partners, and consultants. At first, diverse business objectives of all stakeholders make it challenging for operators to have a single cybersecurity protocol, and then there may be a systemic concern of already-infected rigs and devices entering the ecosystem.[16]

Drilling and computer systems in place, mostly in offshore rigs, were designed around the theory of an isolated network—the notion that the hundreds of miles of ocean and the physical barriers to get to the rig provide a natural defense against cyber-attacks.[17] But with the coming of real-time operations centers—which access and visualize real-time offshore rig data from anywhere in the world, control drilling operations, and even link geoscience and engineering databases and predict drilling hazards—nothing is off the hacker's radar. Additionally, the industry is mechanizing and automating even manual tasks such as the lifting of pipes from racks at a rig (such as Nabors' iRacker), making everything interconnected.[18]

The O&G production operation ranks highest on cyber vulnerability in upstream operations, mainly because of its legacy asset base, which was not built for cybersecurity but has been retrofitted and patched in bits and pieces over the years.

As with the vulnerability factor, the severity of a cyber-attack is highest in the development drilling operation. Whether it is an asset loss, business disruption, regulatory fines, reputation damage, IP theft, or a health, environment, and safety incident, this phase has the highest future opportunity cost across all the risk categories. From hackers drifting a floating unit off of a Gulf of Mexico well site, to tilting an oil rig off the coast of Africa, to making network subject-matter resources take 19 days to delete malware from an oil rig on its way from South Korea to Brazil, the phase has already seen many incidents.[19] In creating new value by adopting open-source, vendor-neutral data protocols (for instance, Wellsite Information Transfer Standard for Markup Language, WITSML), the industry should see that hackers don't use it to their advantage by manipulating this now-comprehensible well data.

The other two main phases of development—field development planning and well completions—have relatively lower cyber risk profiles. Field development planning, in particular, has few real-time connections with other operations but involves cross-disciplines such as geology, geophysics, reservoir management, production, infrastructure, completion, economics, and finance, therefore offering hackers many entry points. Apart from losing the confidential field design data and blueprint of technologies and installations, a hacker making even a small change in the GPS coordinates of rig and optimum well spacing could carry significant financial implications.

The well completion process has a high probability of slipping into the high-risk cyber zone. The industry is aggressively prototyping new and connected technologies to reduce well completion time through real-time monitoring and advanced analytical software, especially in the areas of fracturing fluids, sand, and logistics management in US shales. According to Schlumberger, "the growing intensity of horizontal well programs demands that the next wave of fracturing technology come loaded to bear with sensors and real-time data streaming capabilities."[20]

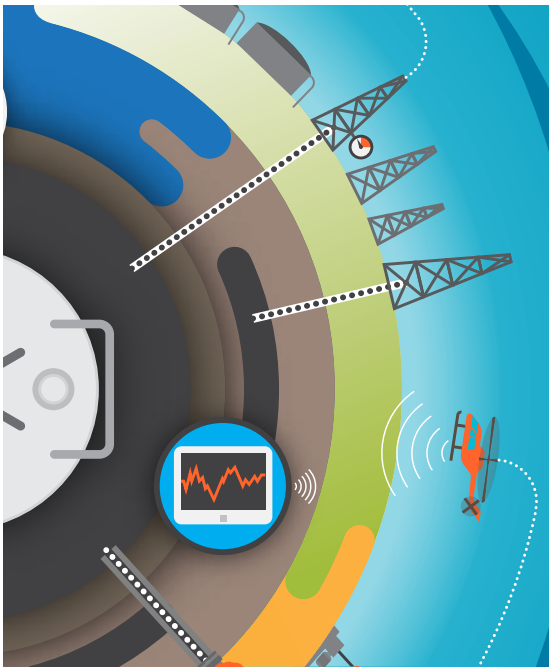
A point worth clarifying: No one should blame automation and connectedness for an increase in O&G cyber risks. Automation makes operations efficient and safer and, very importantly, gives meaningful savings and time back to operators and management, which we worry companies are failing to utilize for safeguarding this new value creation by doing acceptable cybersecurity planning and investments.

3. Production and abandonment

The oil and gas production operation ranks highest on cyber vulnerability in upstream operations, mainly because of its legacy asset base, which was not built for cybersecurity but has been retrofitted and patched in bits and pieces over the years, and lack of monitoring tools on existing networks. Approximately 42 percent of offshore facilities worldwide have been operational for more than 15 years, fewer than half of O&G companies use monitoring tools on their networks, and of those companies that have these tools, only 14 percent have fully operational security monitoring centers.[21]

What explains or magnifies the above cybersecurity problem is an expansive operating environment and the changed role of instrument vendors from system suppliers to system aggregators. A large US O&G company has more than 25,000 producing wells, and each well has a diverse set of industrial control systems—from sensors in boreholes, to programmable logic controllers on a well, to SCADA systems in local control centers—purchased from a number of vendors with different maintenance schedules and connected using off-the-shelf technologies.[22]

On top, these loosely coupled but nonetheless integrated industrial control systems are increasingly connected with a company's enterprise resource planning systems. With 75 percent of global oil and gas production controlled by resource planning systems, this part of the value chain faces cyber risks both from the top (IT systems) and bottom (hardcore legacy operation technology systems in the field).[23] Thus, the consequence of a cyber-attack on



oil and gas production could be severe, promptly affecting both the top and bottom lines. Unlike more complex and specialized seismic and drilling data, production parameters (typically consisting of temperature, flow rate, pressure, density, speed, etc.) are relatively easy to understand, allowing hackers to go for high-consequence breaches.

The last stage of the value chain—well intervention, workover, and abandonment—has a lower vulnerability profile, as the process mostly involves mechanical alteration, well diagnostics, and replacement and maintenance work. But lately, vendors are increasingly using interoperable equipment and standard software platforms and HMI interfaces to reduce costs, which in turn are raising vulnerability risks.

Mitigating cyber risks using a holistic risk management program

ASCERTAINING cyber risks is the first step; forming risk mitigation strategies is the next. The all-too-common response when it comes to mitigating cyber risks is to attempt to lock down everything. But with IoT technology connecting ever more systems and hackers becoming more sophisticated, zero tolerance of cyber incidents is simply unrealistic. Thus, a company should focus equally on gaining more insight into threats and responding more effectively to reduce their impact. Put simply, an effective cyber strategy needs to be secure, vigilant, and resilient.[24]

So for O&G strategists, a question is how to make the most critical operations—seismic imaging in exploration, drilling in development, and well production in production and abandonment (as the above section explained)—secure, vigilant, and resilient. The next section describes three illustrative cyber incidents, one for each of the critical operations, to explain and highlight potential secure, vigilant, and resilient strategies. We assume companies already have standard IT solutions in place so here focus more on strategic solutions.

A company needs a holistic *vigilant* strategy, considering that securing every drilling asset is nearly impossible and additional security features may interfere with the availability of operations or slow down time-sensitive decision making.

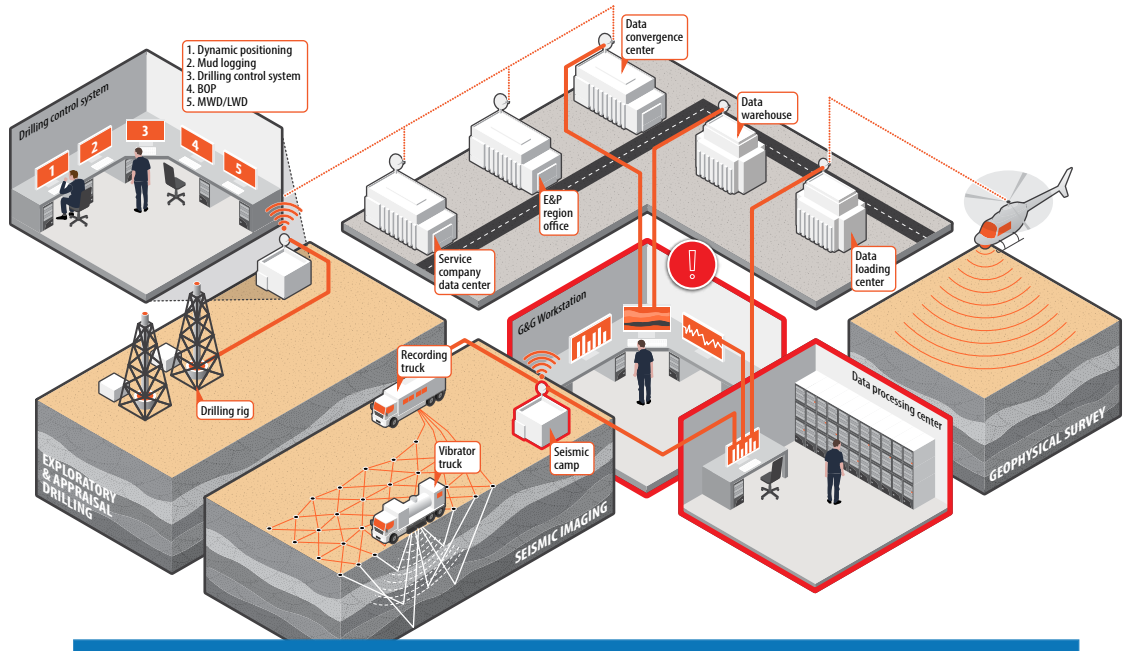
1. Exploration

Scenario: As an offshore seismic imaging project, using a network-attached storage and data management system, nears completion, malware enters through one of the network storage nodes and reaches high-performance computing systems. Although the malware does not impact operations, it steals the competitive seismic data for a field that is up for bidding. How can a company safeguard its digitization drive for seismic data?

Although petabytes of seismic data act as a natural barrier by overwhelming hackers, the growing trend of digitalization and storage of seismic data in the cloud requires *securing* the sub-surface data from industry spies. By substituting each sensitive seismic data element with a nonsensitive equivalent, called a token, and running applications on tokens instead of actual data, a company would offer would-be hackers nothing of value to exploit or steal. The core token generation or indexation system is isolated, and the system stores the actual seismic data in an encrypted format with strong access controls.[25]

As several business disciplines access seismic models throughout the field life cycle, and the models are

Figure 4a. Countering malware



EXPLORATION

THREAT	Malware enters through network storage nodes to steal the competitive seismic data for an offshore field that is up for bidding
SECURE	**Tokenizing** actual seismic data and running applications on tokens
VIGILANT	Monitoring **discipline-level** network traffic
RESILIENT	Setting up a **cluster-based backup architecture** for data stored in multiple storage nodes

Source: Deloitte analysis.

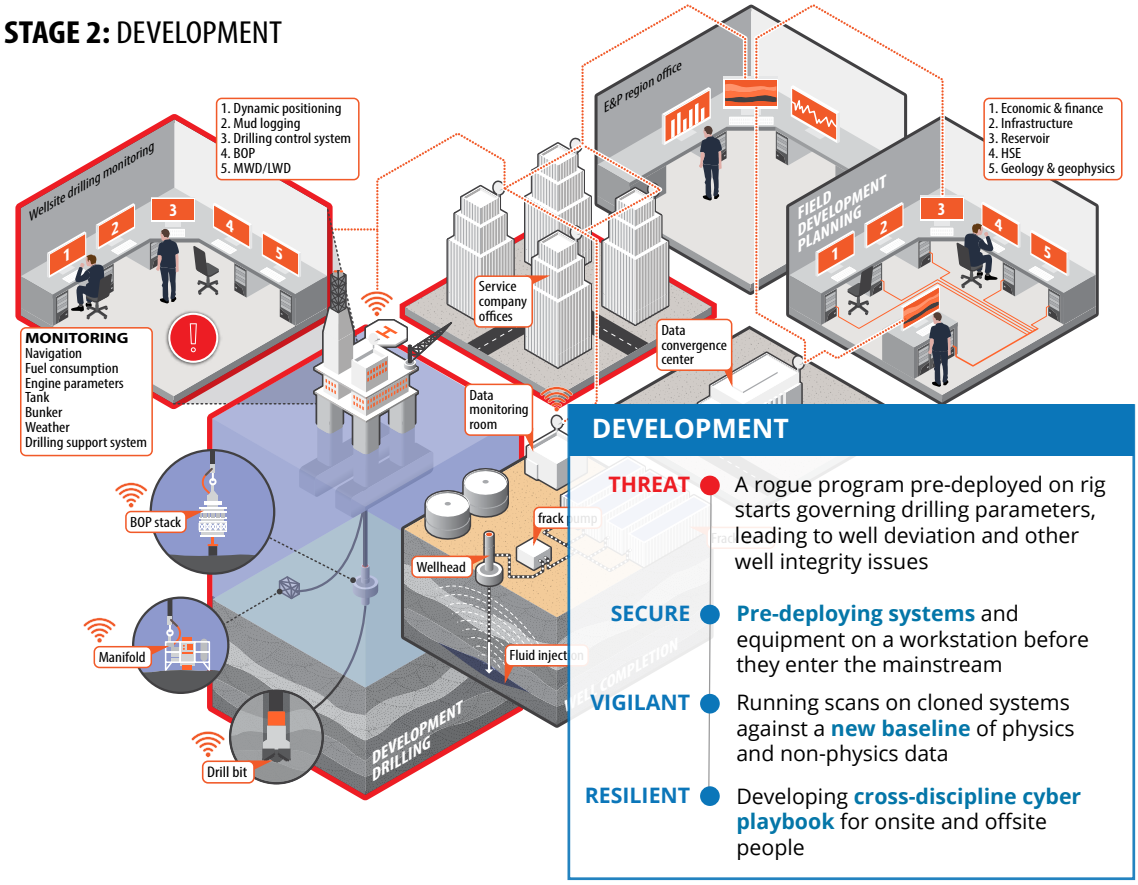
constantly improved with new data from multiple repositories, an O&G company should be *vigilant* about potential data theft. By logging network traffic across disciplines and inspecting it against established baselines for the disciplines—to catch, for instance, a user downloading too much data or gaining access to data unusually frequently—a company can proactively monitor traffic associated with seismic data.[26]

Considering the substantial cost of seismic data acquisition, having a trusted backup of seismic data is essential to ensure that even if the actual data is compromised, the processing and interpretation of seismic data continue or remain *resilient*. With a shift toward digital storage and processing of seismic data using multiple storage nodes, a company's backup workflow also needs to align with this framework. Rather than a monolithic solution that would require time to recover lost data, a cluster-based program that connects each node in the backup cluster to other storage nodes could allow faster data recovery in case of a breach.[27]

2. Development

Scenario: A rogue software program, hiding in a rig component's system or appearing from a network loop, enters the drilling control system and begins governing essential drilling parameters. The result is angular deviation of the well, sudden

Figure 4b. Blocking a rogue program



Source: Deloitte analysis.

fluid influx, and well integrity issues, leading to significant additional costs and putting both people and the environment at risk. How best to avoid or respond?

Considering the complex ecosystem of vendors and equipment in drilling, a company can *secure* its operations by pre-deploying (a.k.a. pre-testing) new systems, equipment, and software before they enter the mainstream system. An operator-governed pre-deployment station on a rig could identify existing malware early and confirm that systems adhere to minimum cyber standards.[28]

A company needs a holistic *vigilant* strategy, considering that securing every drilling asset is nearly impossible and additional security features may interfere with the availability of operations or slow down time-sensitive decision making. By running cyber scans on cloned SCADA and other specific systems rather than on actuals, and by searching for anomalies against a "baseline of normal" using both physics and nonphysics-based data, a company can detect a breach early before it reaches its target.[29]

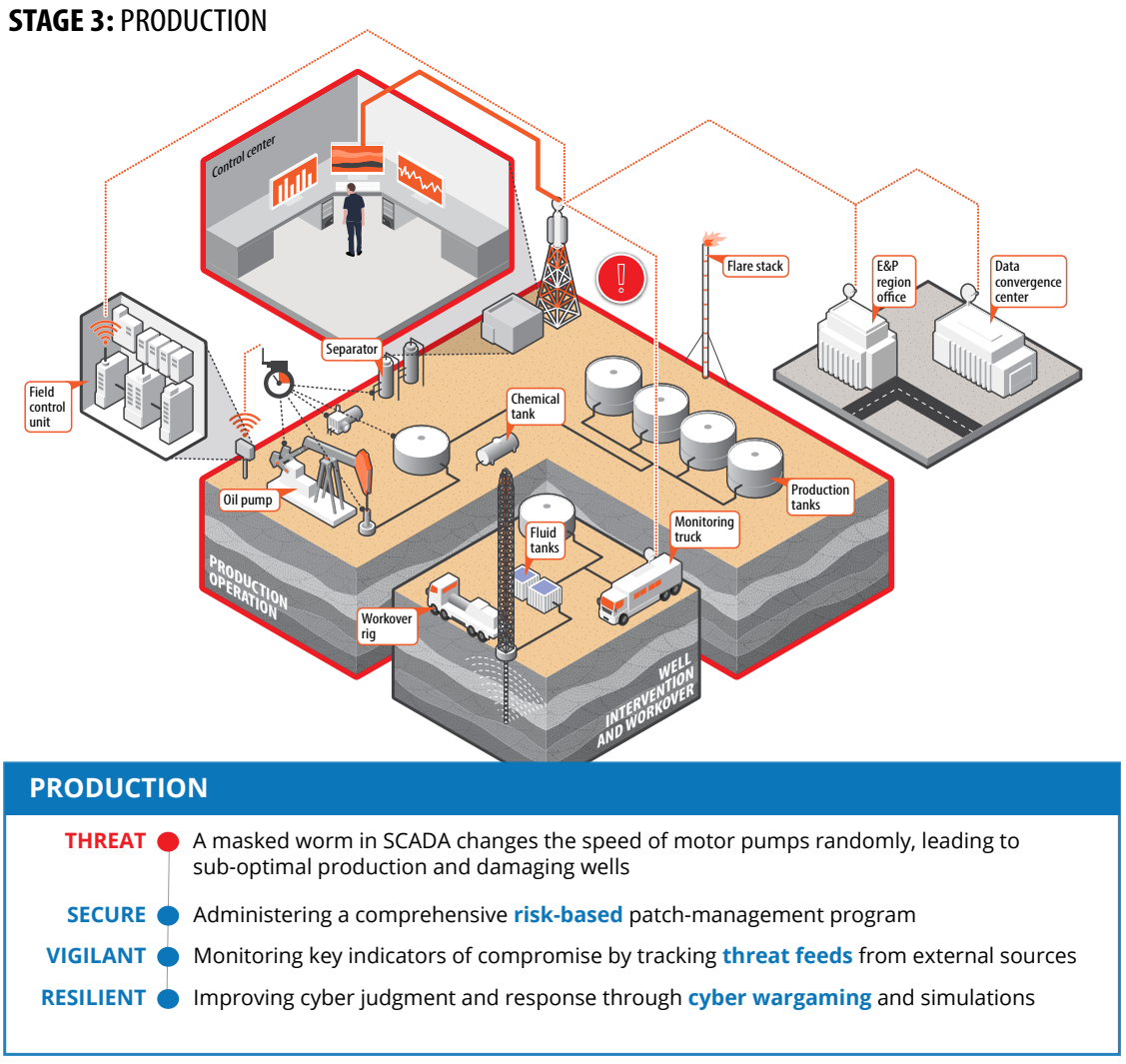
Although creating air gaps or quarantining systems identified as infected is one of the most-used *resilient* strategies, developing a cross-discipline cyber playbook for stakeholders on a rig and onshore control centers could significantly reduce response time and reduce losses.[30] Response time is critical, especially offshore, as daily contract rates for rigs are as high as $500,000.[31] After being overrun by malware, for example, a rig en route from Korea to South America in 2010 had to be shut down for 19 days for engineers to restore its functionality.[32]

3. Production and abandonment

Scenario: A worm is deployed on an onshore industrial control system that can make changes to logics in programmable logic controllers and bypass the protective gearbox for motor pumps. The worm masks the condition of the gearbox in control rooms and changes the speed of the pumps randomly; these variations lead to suboptimal oil production, higher wear and tear of pumps, and even rupturing of wells. What can a company do to avoid such a scenario?

A company can *secure* its critical control systems by administering a holistic patch-management program using a risk-based approach, rather than only following the scheduled or compliance-based approach.[33] At a minimum, this would require inventorying the assets, doing a detailed vulnerability/severity assessment for each asset, and prioritizing and scheduling updates promptly for critical assets. Additionally, an upstream company can err on the side of replacing legacy devices following a

Figure 4c. Stopping a masked worm



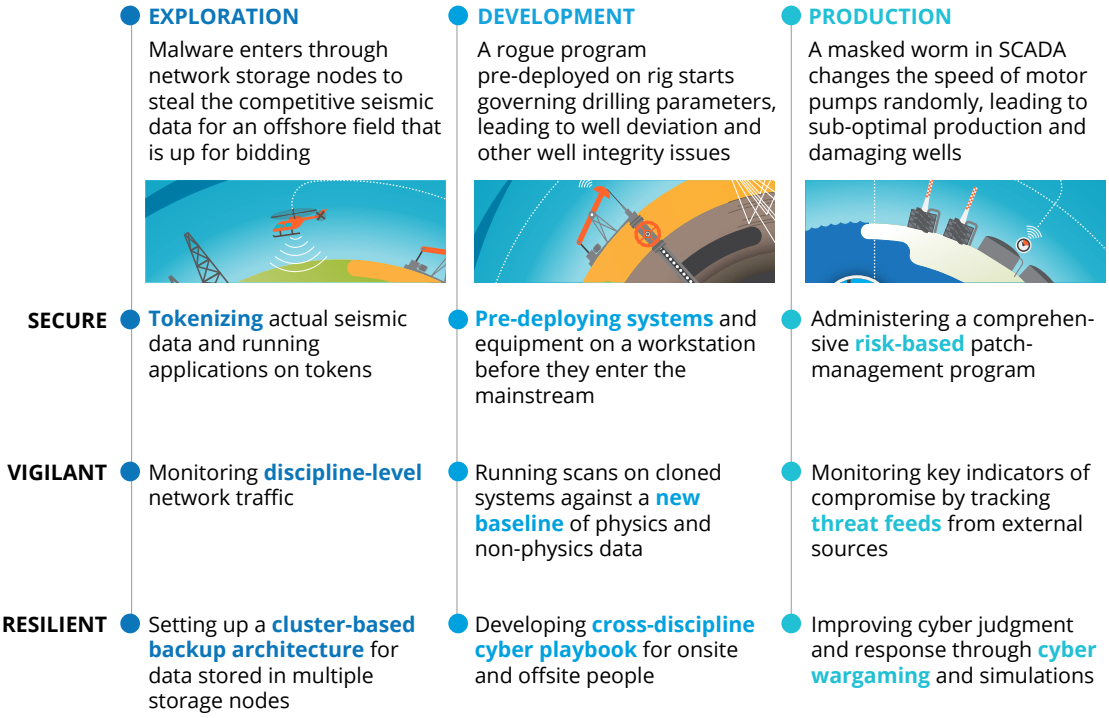
Source: Deloitte analysis.

simple cyber protocol with wholly new purpose-built hardware rather than retrofitting.[34]

By correlating threat feeds from external sources (for example, tracking cyber threat topics and modes on social media) with internal cyber data, a company can elevate its cyber *vigilance* by identifying and addressing threats early. It is essential for an O&G company to share, build, and monitor around key indicators of compromise from external sources, especially knowing that cyber-attacks on the industry's SCADA systems have a long history, with many attacks reemerging in one form or the other—for instance, the second known Shamoon attack in Saudi Arabia in 2016 reused the Disttrack payload method used in Shamoon 1 in 2012.[35]

For rapidly containing the damage, or being *resilient*, a company can regularly practice responding through cyber wargaming and simulations. Staging simulations, especially with people involved in responding to incidents offshore or working in remote locations, creates better understanding of threats and improves cyber judgment at the lowest possible level.[36]

Figure 5: Risk mitigation strategies for cyber incidents on critical upstream operations



Source: Deloitte analysis.

Boardroom buy-in

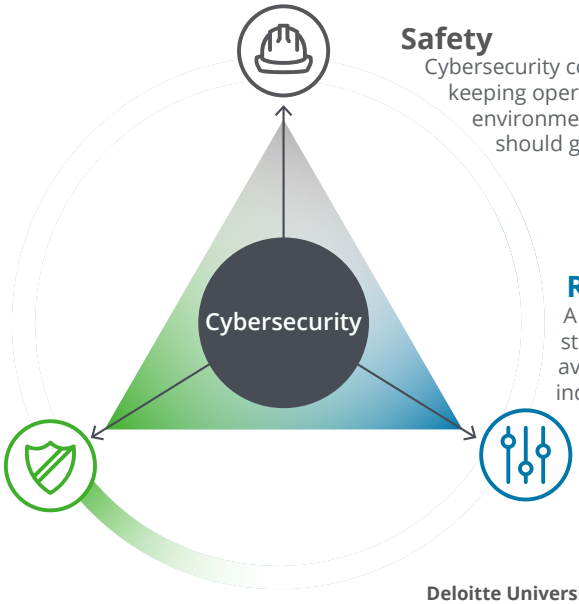
Presenting cyber as a business issue that enables safety, reliability, and value creation

THE upstream oil and gas industry is fast evolving, whereby automation, digitalization, and IoT technology are rapidly integrating into the complex operational ecosystem. However, the industry's march toward interconnectedness has outpaced its cyber maturity, making it a prime target for cyber-attacks. We believe that limited strategic appreciation and sponsorship at a boardroom level—rather than lack of technical know-how—explain the industry's relatively low cyber maturity.

Getting sponsorship from top management requires framing the problem strategically and describing how cybersecurity enables the company's three topmost operational imperatives: safety of assets, people, and environment; an uninterrupted availability and reliability of assets; and creating new value from assets (see figure 6). The next step involves rallying everyone in the enterprise around a holistic cyber risk management program.

The current period of low oil prices has provided upstream companies—weary after years of chasing high growth—with the much-needed breathing space to focus on internal processes and systems. The industry has made a great beginning by focusing on efficiency; now it needs to close by safeguarding operations from cyber-attacks. We believe that cyber, like automation and digital oil fields, can quickly mature from a cost item to an essential investment.

Figure 6. Cybersecurity enables safety, reliability, and value creation



Source: Deloitte analysis.

Appendix

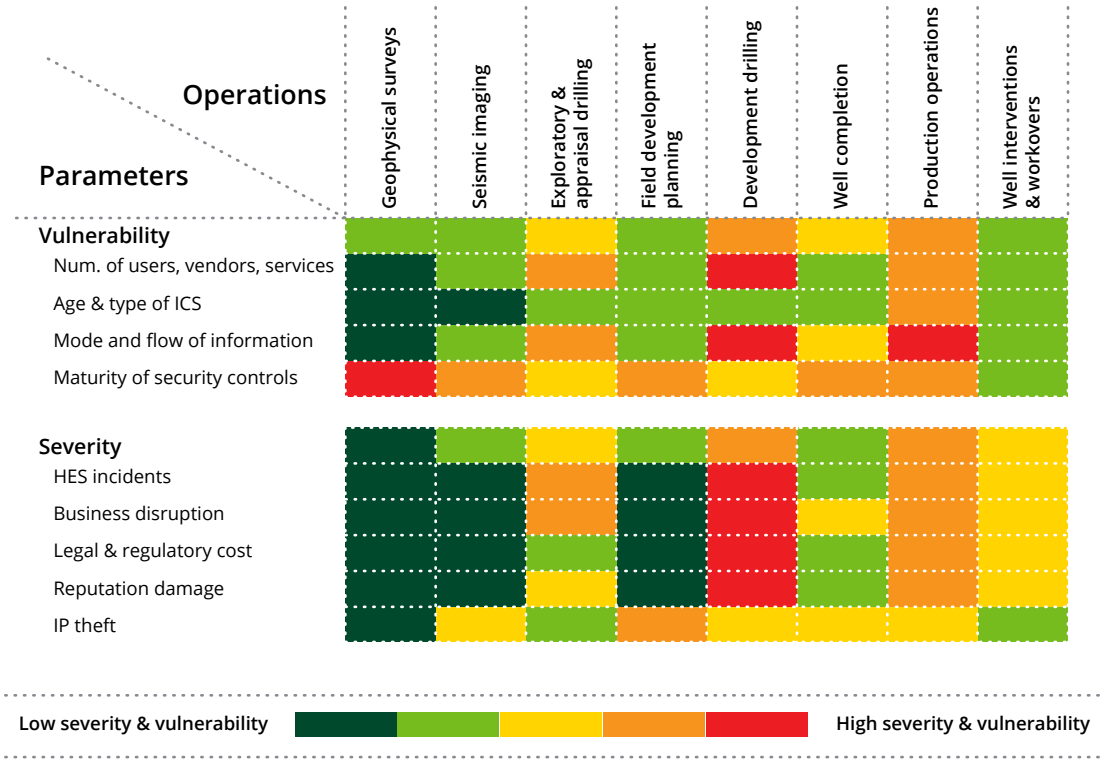
Research methodology

We qualitatively mapped each upstream operation on the cyber vulnerability/severity matrix using a mix of primary interviews, extensive secondary research including a review of technical papers, recent surveys on the industry's cyber preparedness, and study of recent cyber-attacks on a product and service portfolio of oilfield services, automation, and cyber service providers.

For ascertaining cyber vulnerability, we considered aspects such as: number of users, vendors, interfaces, and services involved in each operation; age and type of control systems (legacy, proprietary, open-ended, or close-ended), and working mechanism of software and control systems (default or query-based); mode and flow of information (physical, virtual, mixed); and the maturity of existing cybersecurity controls.

For ascertaining cyber severity, we looked at aspects such as: type of injury (fatal or nonfatal) and probability of a spill, leakage, and pollution; downtime cost; potential fines and penalties by regulators; damage to brand and reputation; and loss of field data and other competitive data.

Figure 7. Cyber vulnerability/severity for O&G operations



Source: Deloitte analysis.

ENDNOTES

1. Paul Zonneveld and Andrew Slaughter, *An integrated approach to combat cyber risk: Securing industrial operations in oil and gas*, Deloitte, May 2017, https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/integrated-approach-combat-cyber-risk-energy.html.
2. Ibid.
3. ICS-CERT, Monitor Newsletters, January to December 2016, https://ics-cert.us-cert.gov/#monitornewsletters; Ponemon Institute, "The state of cybersecurity in the oil & gas industry: United States," February 2017, http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf.
4. Based on the scan of the latest annual filings of top 25 O&G companies worldwide.
5. FireEye, "Cyber threats to the Nordic region," May 2015, www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf.
6. US Department of Homeland Security, "NCCIC/ICS-CER—2015 year in review," https://ics-cert.us-cert.gov/sites/default/files/annual_reports/year_in_review_fy2015_final_s508c.pdf.
7. Jim Finkle, "Shamoon virus returns in new Saudi attacks after 4-year hiatus," Reuters, November 30, 2016, www.reuters.com/article/cyber-saudi-shamoon-idUSL1N1DW05H.
8. Ponemon Institute, "2016 cost of cyber crime study & the risk of business innovation," October 2016, www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.
9. Doug Black, "ExxonMobil, NCSA, Cray Scale reservoir simulation to 700,000+ processors," EnterpriseTech, February 17, 2017, www.enterprisetech.com/2017/02/17/exxonmobil-ncsa-cray-scale-reservoir-simulation-700000-processors/.
10. GlobalData, "Oil & gas database," https://energy.globaldata.com/research-areas/oil-and-gas, accessed on April 15, 2017.
11. *Economist*, "Oil struggles to enter the digital age," April 6, 2017, www.economist.com/news/business/21720338-talk-digital-oil-rig-may-be-bit-premature-oil-struggles-enter-digital-age.
12. Spears & Associates, "Oilfield market report," April 1, 2016.
13. McAfee, "Global energy cyberattacks: Night Dragon," February 10, 2011, www.mcafee.com/hk/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.
14. Intel, "Intel Enterprise Edition for Lustre strengthens oil and gas exploration," 2015, www.intel.com/content/dam/www/public/us/en/documents/case-studies/intel-enterprise-edition-for-lustre-strengthens-oil-and-gas-exploration.pdf.
15. Andrew Slaughter, Gregory Bean, and Anshu Mittal, *Connected barrels: Transforming oil and gas strategies with the Internet of Things*, Deloitte University Press, August 14, 2015, https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-oil-and-gas-industry.html.
16. Linda Hsieh, "Industry recognizing need for better cyber defenses as hackers become more sophisticated and drilling equipment becomes more interconnected," *Drilling Contractor*, September 8, 2015, www.drillingcontractor.org/drilling-cybersecurity-36727.
17. Ibid.

18. Jordan Blum, "Fewer jobs in oil patch as automation picks up," *Houston Chronicle,* December 21, 2016, www.houstonchronicle.com/business/energy/article/Fewer-jobs-in-oil-patch-as-automation-picks-up-10812124.php.

19. Sonja Swanbeck, "Coast Guard commandant addresses cybersecurity vulnerabilities on offshore oil rigs," CSIS, June 22, 2015, www.csis-tech.org/blog/2015/6/22/coastguard-commandant-addresses-cybersecurity-vulnerabilities-in-offshore-oil-rigs.

20. Trent Jacobs, "Schlumberger: New automated hydraulic fracturing tech trims time and workforce requirements," *Journal of Petroleum Technology*, April 6, 2017, www.spe.org/en/jpt/jpt-article-detail/?art=2892.

21. GlobalData, "Oil & gas database"; Tim Heidar, "Digital trenches: On the front lines of the cyber war," Fox-IT, October 14, 2016, www.fox-it.com/en/about-fox-it/corporate/news/65-oil-gas-companies-unprepared-major-cyberattack/.

22. Annual filings of large international oil companies, 2016.

23. SC Media UK, "Black Hat Amsterdam: Oil & gas cyber-vulnerabilities," November 12, 2015, www.scmagazineuk.com/black-hat-amsterdam-oil-gas-cyber-vulnerabilities/article/535118/.

24. Irfan Saif, Sean Peasley, and Arun Perinkolam, "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age," *Deloitte Review* 17, July 27, 2015, https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html.

25. Linda Musthaler, "Are you overlooking tokenization as a data security measure?", *Network World*, November 6, 2015, www.networkworld.com/article/3002307/security/are-you-overlooking-tokenization-as-a-data-security-measure.html.

26. John Kindervag with Stephanie Balaouras, Kelley Mak, and Josh Blackborow, "No more chewy centers: The zero trust model of information security," Forrester, March 23, 2016, www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682.

27. Hari Mankude, "Big Data needs a new backup architecture—part 1," Talena, August 18, 2015, https://talena-inc.com/blog/big-data-needs-a-new-backup-architecture.

28. Hsieh, "Industry recognizing need for better cyber defenses as hackers become more sophisticated and drilling equipment becomes more interconnected."

29. Ibid.

30. Deloitte, *Changing the game on cyber risk: The path to becoming a more secure, vigilant, and resilient organization*, 2017, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf.

31. IHS Markit, "IHS petrodata offshore rig day rate trends," April 2017, www.ihs.com/ja/products/oil-gas-drilling-rigs-offshore-day-rates.html.

32. Jeremy Wagstaff, "All at sea: Global shipping fleet exposed to hacking threat," Reuters, April 23, 2014, www.reuters.com/article/tech-cybersecurity-shipping-idUSL3N0N402020140423.

33. Deloitte, *Changing the game on cyber risk*.

34. Saif, Peasley, and Perinkolam, "Safeguarding the Internet of Things."

35. Robert Falcone, "Second wave of Shamoon 2 attacks identified," Palo Alto Networks, January 9, 2017, http://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified/.

36. Deloitte, *Changing the game on cyber risk*.

ABOUT THE AUTHORS

Anshu Mittal

Anshu Mittal is an executive manager in Deloitte Services LP's Energy & Resources eminence team. Mittal has more than a dozen years of experience in strategic consulting and financial and regulatory advisory across all oil and gas subsectors—upstream, midstream, oilfield services, and downstream. He has authored many publications at Deloitte, including: *Connected barrels: Transforming oil and gas strategies with the IoT*; *Following the capital trail in oil and gas: Navigating the new environment*; and *US shale: A game of choices*.

Andrew Slaughter

Andrew Slaughter is executive director of the Deloitte Center for Energy Solutions, Deloitte Services LP. He works closely with Deloitte's Energy & Resources leadership to define, implement, and manage the execution of the Center's strategy; develop and drive energy research initiatives; and manage the development of the Center's eminence and thought leadership. During his 25-year career as an oil and gas leader, Slaughter has occupied senior roles in both major oil and gas companies and consulting/advisory firms.

Paul Zonneveld

Paul Zonneveld leads Deloitte's Global Risk Advisory team for Energy & Resources, including oil and gas, mining, and power and utilities. He specializes in cybersecurity and enterprise risk management, with a focus on strategy, design, and implementation of security solutions to address emerging threats.

ACKNOWLEDGEMENTS

The authors would like to thank executives from **Siemens AG** and **Honeywell International Inc.** for sharing their valuable insights.

Special thanks to **John England** (vice chairman and US Energy & Resources industry leader, Deloitte LLP), **Vivek Bansal** (senior analyst, Deloitte Support Services India Pvt. Ltd.), **Kartikay Sharma** (senior analyst, Deloitte Support Services India Pvt. Ltd.), **Kevin Urbanowicz** (senior manager, Deloitte & Touche LLP), **Matthew Budman** (manager, Deloitte Services LP), and **Alok Nookraj Pepakayala** (senior analyst, Deloitte Support Services India Pvt. Ltd.) for their contributions in research, analysis, review, and design.

CONTACTS

John England
Vice chairman
US Energy & Resources leader
Deloitte LLP
jengland@deloitte.com
+1 713 982 2556
@JohnWEngland

Adnan Amjad
Partner
Cyber Threat Risk Management practice
Deloitte & Touche LLP
+1 713 982 4825
aamjad@deloitte.com

Edward W. Powers
National managing principal
Cyber Risk Services
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

GLOBAL CONTACTS

Anton Botes
Global leader, Oil & Gas
Deloitte Touche Tohmatsu Limited
+27 11 806 5197
abotes@deloitte.co.za

Paul Zonneveld
Risk advisory leader
Global Energy & Resources
Deloitte Canada
+1 403 503 1356
pzonneveld@deloitte.ca

Dina Kamal
Risk advisory leader
National Energy & Resources
Deloitte Canada
+1 416 775 7414
dkamal@deloitte.ca

Amir Belkhelladi
Partner, risk advisory
Deloitte Canada
+1 514 393 7035
abelkhelladi@deloitte.ca

Tiaan van Schalkwyk
Associate director, risk advisory
Deloitte Africa
+27 11 806 5167
tvanschalkwyk@deloitte.co.za

Rajeev Chopra
Global leader, Energy & Resources
Deloitte Touche Tohmatsu Limited
+44 20 7007 2933
rchopra@deloitte.co.uk

Steve Livingston
Risk advisory leader
National Power & Utilities
Deloitte US
+1 206 716 7539
slivingston@deloitte.com

Ramsey Hajj
Senior manager, risk advisory
Deloitte US
+1 561 962 7843
rhajj@deloitte.com

Marko Van Zwam
Partner, risk advisory
Deloitte Netherlands
+31 88 288 0890
MvanZwam@deloitte.nl

Stewart Davidson
Director, risk advisory
Deloitte UK
+44 20 7303 2178
stdavidson@deloitte.co.uk

Rob Hayes
Director, risk advisory
Deloitte UK
+44 20 7007 2606
rjhayes@deloitte.co.uk

 Follow @DU_Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

About Deloitte