Deloitte.
Insights

Refining at risk

Securing downstream assets from cybersecurity threats

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.

CONTENTS

Introduction | 2

Maximizing opportunities and reducing risks in the rapidly digitizing oil industry | 3

Getting started: Identifying risk through the value chain | 6

Next steps: Building a framework to assess, prevent, and mitigate cyber risks | 10

Going forward: Investing in cybersecurity to enable a more connected O&G future | 14

Endnotes | 15

Introduction

The rewards and risks of connected technology

TODAY'S oil and gas companies rely on industrial control systems to maintain safe and reliable operations, and that's unlikely to change. But companies are increasingly integrating connected technology, making those systems faster and more efficient—and, inevitably, creating openings for potential cybersecurity breaches.

The future increasingly appears to be one in which O&G companies will rapidly integrate robotics, analytics, and the Internet of Things (IoT) into the operational environment, for good reason: Increasing connectivity has the potential to drive value creation by deploying data and analytics to find new markets, improve operational performance, and streamline the supply chain. A more connected oilfield, pipeline, or refinery, though, is potentially a more vulnerable one, and executives need to plan ahead.

As risks grow, each company will need to adapt its own digital strategy, in an industry whose approach to cybersecurity is less mature than it should be.[1] Moving away from one-off, ad-hoc approaches and developing optimized behaviors and controls will be critical to protect existing assets from new threats. In a prior article, *An integrated approach to combat cyber risk: Securing industrial operations in oil and gas*,[2] we outlined a number of these threats facing the industry as well as steps to identify, evaluate, and minimize them. We later drilled down into the upstream industry in *Protecting the connected barrels: Cybersecurity for upstream oil and gas*,[3] identifying key risks that explorers, drillers, and producers face.

This article focuses on the challenges facing the downstream industry across a number of businesses, including supply and trading, refining, distribution, and retail. It offers a framework to assess risks and develop next steps to prevent or mitigate them. And it outlines a plan of attack for key stakeholders to implement new protocols to create a more secure, vigilant, and resilient enterprise.

Maximizing opportunities and reducing risks in the rapidly digitizing oil industry

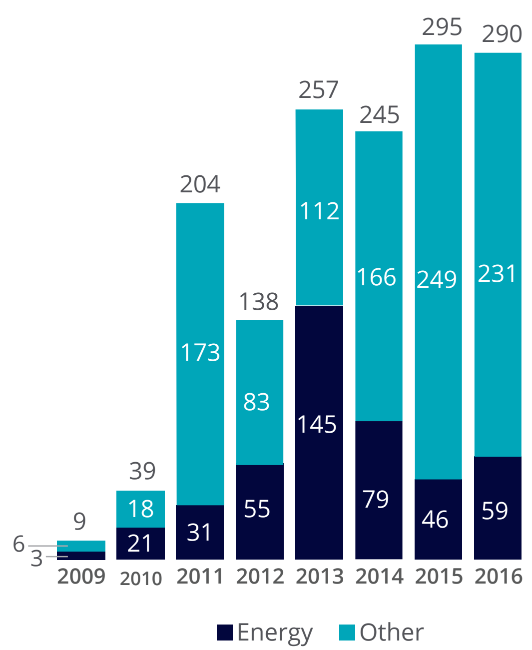
PIPELINES, refineries, and tank farms all rely heavily on industrial control systems (ICS) to maintain smooth, safe operations. With advances in sensor technology, processing power, and remote operational capabilities, IoT technology could unlock tremendous value by eliminating redundancy, increasing uptime, and more promptly allocating feedstocks, plant utilities, and products, while reducing costs.[4] However, the IoT poses not just opportunities for increased efficiency through smarter systems management—its connected systems increase security risks and consequences. This concern is not just academic: Hackers have initiated hundreds of cybersecurity incidents targeting US O&G control systems (see figure 1), many with significant real-world impacts.[5]

At this point, the hazards are largely speculative: To date, there is limited evidence that cyber-attacks in the O&G sector have caused large-scale incidents at either upstream production plants, downstream refineries, or the infrastructure such as pipelines and storage facilities connecting the two. However, a number of suspicious incidents offer ample incentive for caution. A 2008 explosion in a Turkish pipeline was originally believed to be caused by Kurdish separatists and later a cyber-attack, though lack of evidence makes fundamental attribution difficult.[6] In 2015, a number of petrochemical fires in the Middle East raised suspicions that computer viruses had compromised equipment.[7]

Outside of oil and gas, but perhaps more relevant to refiners, is the 2014 cyber-attack on a German steel mill that led to loss of control of a blast furnace, subsequently causing significant damage to the plant.[8] The incident stands out for three things:

- It was one of the first verified attacks to cross the cyber/physical barrier to cause real-world damage;
- The incident originated with an ordinary spear phishing-type intrusion (originating with a bogus email purporting to be from a trusted source) that migrated from the business systems to the industrial control systems;

Figure 1. ICS-targeted cyberattacks disproportionately affect oil and gas companies



Source: Deloitte analysis, Industrial Control Systems Cyber Emergency Response Team, *Houston Chronicle.*

Deloitte Insights | Deloitte.com/insights

- The attack affected the furnace controls—similar to the systems that typically interface with equipment in many downstream operations.

It is not hard to imagine how a similar attack might target a refinery, leading to tank overflow, vessel rupturing, or even an explosion. While health, safety, and environmental risks are naturally at front of mind, companies face financial risks as well, beyond cleanup and lawsuits. A disruption in a pump network might not lead to widespread damage but could require equipment replacement and would likely idle both staff and equipment. There could be a long tail of lower-impact events. This is particularly true for the downstream, as refining relies heavily on automation, sensors, and controls systems.

For example, a loss of a single day of operations for a 100,000 barrel-per-day refinery could reduce revenue by over $5.5 million and profit by $1.4 million.[9] The United States has more than 140 refineries, with total daily capacity exceeding 18 million barrels, all of which could be potentially vulnerable.[10] If a cyber-attack spread from one facility to another, or down the value chain affecting distribution and retail networks, it could potentially lead to tens of millions of dollars of lost revenue. In addition, any physical damage could potentially inflict millions (if not billions) of dollars of repair and construction costs. In a more connected world with connected sensors, higher-level automation, and less direct human control, that broader impact becomes increasingly more likely and more consequential.

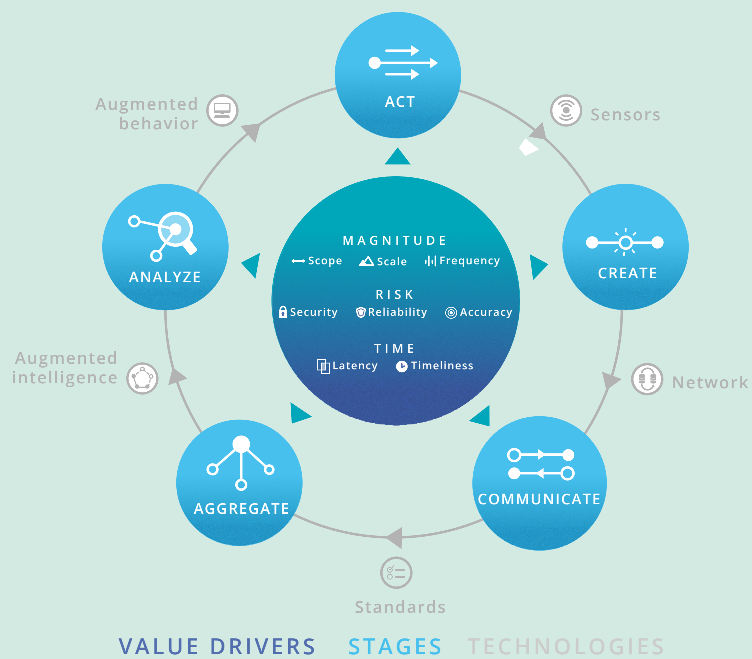
For companies operating downstream assets—not just refineries but the storage, pipeline distribution, and retail networks that support them—cyber threats remain a high-potential and high-frequency risk. With the number of attacks on nonpetroleum infrastructure rising and clear parallels to similar process systems used within oil and gas, companies need to take proactive steps to identify and reduce existing risks.

CONNECTED TECHNOLOGY MOVES DOWNSTREAM

At the most basic level, the Internet of Things refers to increased connectivity between consumers, objects, and the companies that manufacture them, ranging from something as mundane as a home refrigerator to highly specialized drilling equipment used offshore in oil and gas.[11] That connectivity, with sensors generating oceans of data and systems interpreting the information, both opens up possible ways of creating significant future value and represents new sources of cybersecurity vulnerabilities.

In oil and gas, IoT technology has already demonstrated potential for increasing production, reducing costs, and improving safety. For example, predictive maintenance in the downstream could provide two benefits: accurately spotting equipment failure ahead of time and identifying wear levels independently for each component, which could save time and money by allowing companies not replacing equipment in good condition even if its operational time has exceeded standard preventative maintenance schedules. The IoT's value is derived by creating a virtuous cycle (see figure 2) in which data is collected across a network of machines and sensors and aggregated and analyzed, thus allowing for quicker (even real-time) decision-making based on facts on the ground, not just industry heuristics or armchair theorizing. However, each sensor, and each point connecting that sensor to a monitoring system, represents a potential attack surface for outside threats.

Figure 2. How IoT technology can add value to oil and gas



Source: Deloitte analysis.

Deloitte Insights | Deloitte.com/insights

Outside of the refinery, the challenges could increase. In the case of supply chain management, IoT applications could enable adapting just-in-time approaches to refining and petrochemicals by adjusting to real-world buy signals identified by advanced algorithms—thus reducing excess feedstock and unsold end products and maximizing pricing. Similarly, that algorithmic analysis could be applied to distribution by optimizing product mix and vehicle routes, resulting in improved utilization. Combining disparate technologies such as GPS tracking, machine learning, and data scraping has a lot of potential to remove waste from the entire value chain. In a margin-driven business such as downstream oil and gas, IoT-enabled efficiencies could translate into a long-term strategic advantage for companies that get it right. To make this new approach work, companies will likely look to connect plant-wide processes, external databases, and vehicle-tracking information through a central analytics-type function. As the number of connections increases, the likelihood and severity of intrusions would likely grow exponentially, making security critical for deployment.

Because of the value that IoT technology can potentially deliver, it is important for companies to build flexibility into their cybersecurity programs. Connecting sensors and controls systems carries inherent risks—particularly if both are also connected to external networks—but restricting or blocking interconnectivity will undermine potential value creation. Therefore, information technology (IT) and operational technology (OT) stakeholders will likely need to identify—quantitatively, if possible—the risks and benefits of leveraging new technologies. In some cases, traditional methods may work best. However, the potential for risk is a weak argument for maintaining the status quo. Ultimately, achieving an appropriate balance between risk and reward will be key.

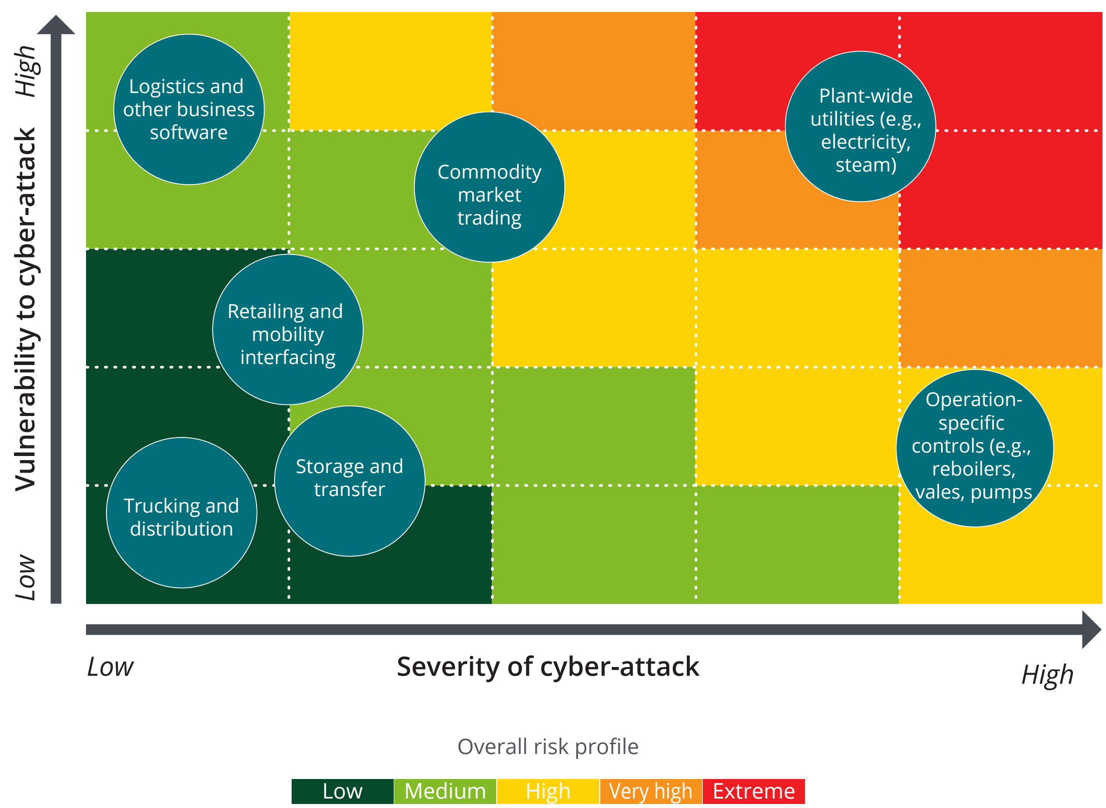
Getting started

Identifying risk through the value chain

RISKS stem from a number of sources and vary substantially by process, company, and geography. At its core, risk comprises two factors: probability and impact. In the case of cybersecurity, the primary interest is in likelihood of intrusion, determined in part by the target's attractiveness and the number of attack surfaces. Impact is determined by what that vulnerability is connected to, whether it is as ubiquitous as an email server or as specialized as a distillation column's reboiler. Companies must consider both the likelihood of attack (in other words, vulnerability) and the type of impact (in other words, severity) when analyzing cybersecurity challenges.

Using risk matrices that are common to industry is one way to conduct those assessments. In this case, companies can prioritize processes by risk level and develop the appropriate scope for future prevention and mitigation (see figure 3). Ranking each process or grouping by both vulnerability and severity provides a road map to discuss not just individual risks

Figure 3. Indicative risk assessment for key downstream functions and operations



Source: Deloitte analysis.

Deloitte Insights | Deloitte.com/insights but also overarching corporate strategic risks affecting future capital investment and operational flexibility. Moreover, establishing this kind of familiar framework can help get buy-in from both IT and OT upfront, which will likely be critical for long-term success.

These risks are unequally distributed across the downstream (see figure 4). Obviously, the most important include processes related to safety equipment; high-pressure and high-temperature processes could lead to high-impact negative events. For example, losing control of coolant pumps or reboilers could lead to unplanned equipment failure or potential chemical ignition. Plant utilities pose the same issues, only magnified. Loss of electric power, cooling water, or steam generation could lead to the same fire hazards, as well as refinery-wide shutdowns. Moreover, connected technology will likely link plant-level processes with more cyber/physical interfaces, elevating vulnerability.

> Companies must consider both the likelihood of attack and the type of impact when analyzing cybersecurity challenges.

Logistical software, on the other hand, may pose less risk, limited to delays and communication challenges, but could be more exposed to outside systems and third-party personnel. In some cases, both the vulnerability and impacts are minimal (or can at least be made so). Using manual valves and inherently safe design practices would likely reduce cybersecurity risks for storage and transfer processes—at the expense of potential efficiencies. The same can be said for trucking and distribution racks, provided those systems are separate from those of an associated refinery or petrochemical plant. However, with self-driving vehicles and end-to-end process automation on the horizon, companies may need to continually reassess vulnerabilities.

Interconnectedness also plays a major role in determining likely event severity. Even high-probability and low-impact events could spill over into more sensitive operations. In some cases, where an

Figure 4. Examples of potential downstream cybersecurity risks through the value chain

Business function	Supply and trading	Refinery operations	Logistics and management	Storage and transfer	Distribution	Retail
Scenario	Tampering with market data and transaction systems	Unauthorized shutdown of plant utilities control system	Theft of inventory data on crude oil and refined products	Unauthorized access to and manipulation of pipeline systems	Loss of trucking dispatch information	Theft of customer credit card and sales data
Risk	Increased financial risk exposure, loss of revenue, failure to meet business commitments, and reputational damage	Explosion, loss of materials, equipment damage, and unsafe conditions for personnel and adjacent populations	Reputational damage and failure to meet business commitments	Explosion, spillage, environment damage, and unsafe conditions for personnel and adjacent populations	Loss of revenue, reduced utilization of distribution network, failure to meet business commitments, and reputational damage	Financial liabilities, increased regulatory oversight, and reputational damage

Source: Deloitte analysis.

Deloitte Insights | Deloitte.com/insights

incident is contained, the vulnerabilities are independent of one another. There also can be systemic risks, in which a vulnerability or intrusion in area spreads to other processes. All of these issues (and underlying variables) need to be aggregated, analyzed, and assessed to determine ultimate business risks. The challenges for a large integrated downstream business can be quite complex, and adequate review, identification, and documentation of risk is a key first step.

One thing stands out: These risks are present throughout the value chain. As seen in *An integrated approach to combat cyber risk*, there are a number of potential threats in the upstream, midstream, and downstream segments. Furthermore, the specific risks facing explorers, drillers, and producers outlined in *Protecting the connected barrels* have much in common with those highlighted here in the downstream. In other words, the same vulnerabilities found on a production platform or for a pipeline can be found in the downstream as well—though, of course, the specific business function will differ. Since these challenges transcend specific business functions and industry segments, O&G companies need to take a holistic approach to risk assessment.

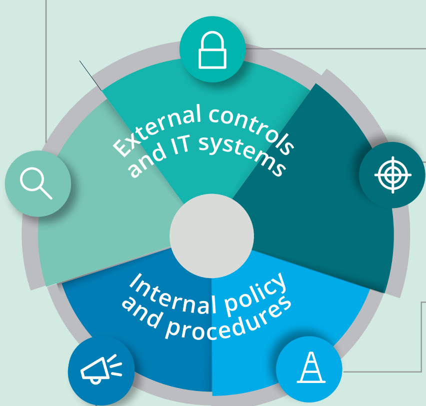
WHAT MAKES THE DOWNSTREAM VULNERABLE TO CYBER-ATTACKS?

Naturally, those outside the O&G industry might envision it as powered entirely by heavy machinery and hard work—whatever gets crude from the ground to the pump. But the sector is becoming increasingly high-tech: Operators appear to be more broadly adopting IoT-type technologies to deliver value, maximize their existing assets, and optimize operations across the value chain.[12]

In the case of the downstream, equipment such as valves, pumps, and compressors, not to mention entire separation and reaction trains, are monitored and controlled by sensors, algorithms, and set points, with human operators inputting parameters and supervising operations. Over time, the process has become more complex, with an increasingly interconnected architecture. Moreover, linking business and technical processes may make sense from an operational standpoint, but that connectivity can provide additional attack surfaces and allow vulnerabilities in one system to expose large parts of a facility to an attack. Increased overlap between IT and OT processes could lead to increased gaps, so multiple layers of processes require multiple layers of controls. A robust defense model outlines the different sources of risk throughout the business and potential controls to mitigate risk (see figure 5). This barrier approach demonstrates the wide array of potential threats and how deeply they can penetrate.

Figure 5. Defense in depth can minimize cyber threat vulnerability

Layered security approach for vulnerability risk assessments



IDENTIFY: Companies need to address all external access points, including all authorized and unauthorized software and devices. They should also consider remote and third-party access, BYOD policies, and physical perimeters (e.g., fences and gates).

PROTECT: Companies need to protect the perimeter by restricting remote access, limiting the use of administrative privileges, and segregating the networks (e.g., ICS versus business). They should air-gap critical processes from the rest of the network.

DETECT: Companies should detect cyber intrusions as quickly as possible by monitoring external access points and checking IT and OT activity against expected baselines. For example, ICS firewalls are key for maintaining downstream facilities.

RESPOND: Companies should develop business continuity and disaster recovery plans. It is important to assess potential damage and isolate any affected systems with the goal of returning to normal operations as soon as possible.

RECOVER: If a cyber threat is identified, key personnel should respond rapidly to limit the impact on affected systems and prevent its spread. Regular review of historical intrusions and current processes will help companies to prepare for future attacks.

Source: Deloitte analysis.

Deloitte Insights | Deloitte.com/insights

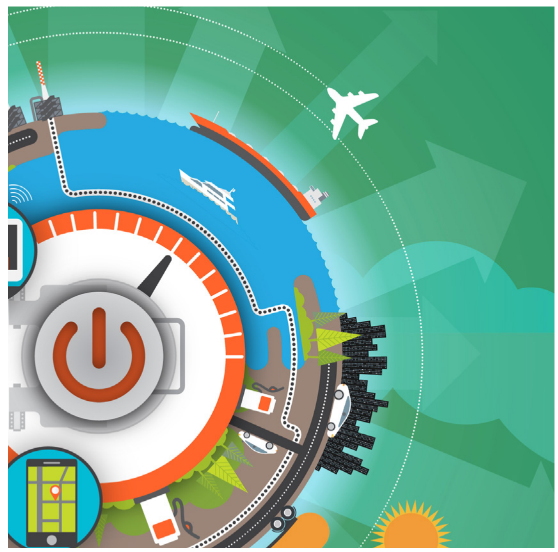
Reducing those risks will become increasingly important in the near future as companies embed digital technology in operations. Refineries, pipelines, and distribution networks already include a number of digital and physical assets, ranging from off-the-shelf logistics software to the tanker trucks delivering fuel to retail stations. Today's interfaces might include a temperature sensor feeding back data to a cooling system's pumps, but in a more interconnected world, it is not hard to imagine that a smart refinery could bypass human supervision to manage its own feedstock levels, product yields, and distribution based on operational and market conditions and constraints (for example, crude oil and gasoline price spreads). And yet the challenges of installing new hardware and implementing new software in a piecemeal fashion from multiple vendors will persist.

Next steps

Building a framework to assess, prevent, and mitigate cyber risks

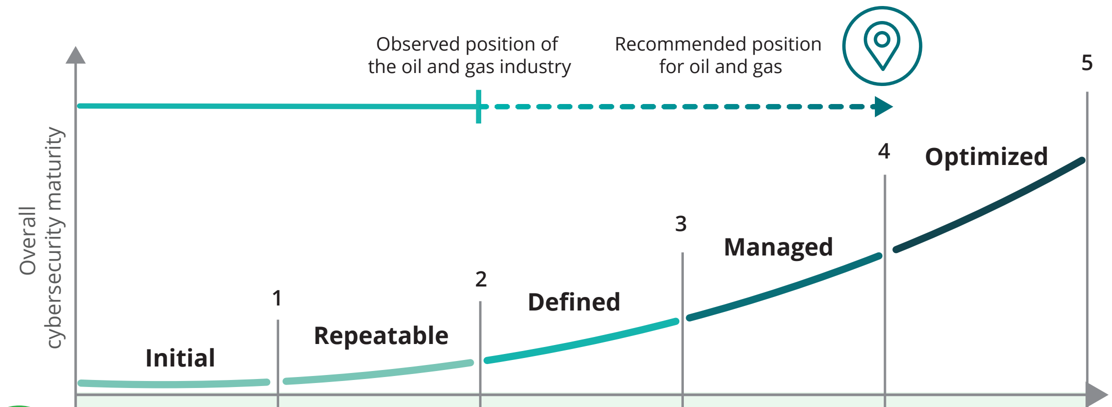
ONCE companies have identified risks, they need to develop a framework to outline their overall cybersecurity strategy. Two considerations stand out. First, companies need to make operations secure, vigilant, and resilient.[13] Broadly speaking, this means identifying the key building blocks to control risks across refineries and business units as well as developing the corporate-level strategy needed to implement them.[14] Second, and in combination with the first consideration, these companies need to make sure that they have in place the right people, processes, and technology. While this may seem more tactical than strategic, it is imperative to take those building blocks and turn them into actionable steps to handle cybersecurity issues. One framework that can address both is the cybersecurity maturity model (see figure 6). It identifies relative maturity levels of behaviors and key controls that should be in place to decrease potential risk. As companies mature, they need to move from one-off solutions to ones that fully address a full range of risks while reducing potential gaps.

There are some ad-hoc approaches to dealing with potential threats with limited documentation, standards, and testing but that many companies lack thorough security plans that rely on clear processes, processes, and analytical capabilities.



What does this model mean in practice? As companies identify new vulnerabilities and risk to business-critical operations, their defenses need to adapt. Based on a number of maturity assessments that Deloitte has performed for a broad range of energy and resources companies, the O&G sector as a whole is about 2.5 on a 1-to-5 scale. That means there are some ad-hoc approaches to dealing with potential threats with limited documentation, standards, and testing but that many companies lack thorough security plans that rely on clear processes and analytical capabilities. We recommend that O&G companies reach or exceed 4 on this scale.[15] Taking into consideration people, process, and technologies, there are a number of steps that

Figure 6. Applying the cybersecurity maturity framework to downstream operations



	Initial	Repeatable	Defined	Managed	Optimized
Behaviors	Dependent primarily on individuals and isolated practices New or relatively inexperienced security team	Ad-hoc approach with some tools and documented procedures Established security function	Clearly defined strategy supported with tools and methods to manage risk Security processes defined and in place Established security function with integrated systems designed to predict, prevent, detect, and respond	Established security capability, with defined processes and measures Focused on risk management and business enablement Two-plus years operating with defined processes and practices	Risk sensing and predictive analytics used to model threats Highly automated Five-plus years operating without a significant failure
Key controls	General awareness of ICS cybersecurity needs but not considered a priority	ICS cybersecurity strategy and policy established Awareness and education Segmentation of ICS and corporate networks Annual risk assessment with identified gaps and remediation plan Physical security	Inventory of all cyber assets Security standards development Annual vulnerability testing 24/7 security monitoring Incident response plan developed and tested Virus and malware protection	ICS secured according to security standards Identity and access management for provisioning and authentication End point security Mobile protection Third-party security	Cyber threat intelligence/ sensing Data loss prevention Behavioral analytics

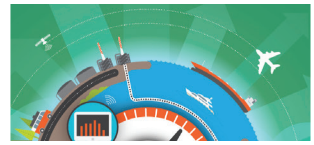
Source: Deloitte analysis.

Deloitte Insights | Deloitte.com/insights

companies can take to increase cybersecurity maturity (see figure 7) and create more secure, vigilant, and resilient downstream operations.

Security, vigilance, and resilience are shorthand for the ultimate end goal for a cyber risk prevention and mitigation program. A *secure* system is one that has minimal exposure to potential cybersecurity breaches. Following the principle that an ounce of prevention is worth a pound of cure, companies should consider isolating potential attack surfaces, limiting unnecessary system interconnections, and restricting access to those who have been well vetted and properly trained. For example, refineries should consider separating business and operational systems. In some cases, companies should

Figure 7. Next steps to increase a company's cybersecurity maturity level

	PEOPLE	PROCESSES	TECHNOLOGY
			
SECURE	Evaluating employees and vendors for **cyber risk potential**, including screening for malicious actors	**Restricting and documenting** access to control systems and other high risk cyber/physical interfaces	Air gapping or otherwise separating high-risk processes, including **plant-level IoT infrastructure**, from the business network
VIGILANT	Implementing security awareness training for all employees, not just those directly involved with **sensitive systems**	Designing **triage protocols** to systematically identify potential cyber incidents and assess risk severity	Deploying **automated monitoring software** to identify potential breaches or equipment mis-operation/-failure
RESILIENT	Developing incident response and **forensic training** for key IT and OT personnel to reduce impact and prevent future incursions	Expanding management of **change protocol** to include cybersecurity impacts from operational and business shifts	**Building redundancy** into key processes through duplication of physical equipment, cyber/physical interfaces or backups of software

Source: Deloitte analysis.

Deloitte Insights | Deloitte.com/insights

consider isolating critical process control loops altogether.

A *vigilant* system is one that has the appropriate tools to monitor processes and identify intrusions. Something as complex as the downstream value chain requires more than the traditional firewall. One approach could be to take advantage of increasingly available connectivity and computing power to build automated security systems. Ideally, they would possess the ability to assess risks on their own, determining which issues could be fixed by the system itself and alerting cybersecurity professionals about the rest.[16] Digital twins could play an important role, particularly for high-risk operations. A digital twin is simply a digital form of a physical asset, with virtual equivalents of engineering content, operating parameters, physical constraints, and uncertain elements.[17] Deploying software that compares actual sensor data in a distillation column or a transfer pump to the twin's simulated values could flag abnormalities in real time. Moreover, this could identify not just cyber-attacks but physical operational failures as well.

Companies should consider isolating potential attack surfaces, limiting unnecessary system interconnections, and restricting access to those who have been well vetted and properly trained.

Last, a *resilient* system has the capacity to operate continuously despite intrusions. Training employees to identify and isolate compromised systems and processes is a good starting point. Redundancy will likely be key, since maintaining backup systems could provide fast restart capabilities following the elimination of a threat. Inherently safe design combined with manual bypasses could play a role as well. For logistics or commodity trading, duplication of data may be critical. Outsourcing functionality to external cloud computing might be one solution. Using the cloud could provide flexibility and scalability as well as reduced costs and external security.[18] However, for remote operations or those lacking secure Internet access, cloud computing could create reliability issues for critical path-dependent operations as well as create new sources of third-party risk.

Executing a secure, vigilant, and resilient security strategy will require people to be on the same page, processes to be set up and well documented, and new technology deployed where appropriate. If personnel are inadequately trained, if software is dated, or if a company uses a patchwork of conflicting processes, vulnerabilities will be exposed and threats will have a higher likelihood of compromising operations.

Going forward

Investing in cybersecurity to enable a more connected O&G future

ONCE a company identifies key cybersecurity risks and develops an analytical framework, it needs to take action. Two major barriers that O&G companies potentially face are a lack of awareness and a lack of coordination.[19] Additionally, there can be concerns about cybersecurity talent shortage and implementation costs.[20] Unsurprisingly, planning will be key for success. Even with a solid plan in hand, executive sponsorship and buy-in from all affected parties will likely be equally important to move from ideation to implementation.

Defining the scope of vulnerabilities upfront can both raise awareness of cybersecurity risks and serve as a focal point to align both IT and OT organizations within a company. Using a risk matrix such as shown in figure 3 as part of the conversation can highlight where risks are clustered. In this example, downstream functions were categorized, but the same approach could be used to analyze geographical or business groupings. From there, IT and OT can list mission-critical business processes (on the operational side) as well as inventory cyber and cyber/physical interfaces (on the technology side).

As with the scoping process, using a framework (for example, the cybersecurity maturity model) to outline next steps can also bring together the key stakeholders across the organization. For example, if the company identifies personnel as a potential vulnerability, executives from across the talent, training, and IT organizations can come together to develop new training programs to increase cyber awareness. Alternatively, if internal expertise is lacking, the project sponsor can identify vendors to meet the need. Deciding those next steps early on will likely make implementation smoother.

From there, the project sponsors can build a plan of attack and finalize the project management details (for example, cost, timeline, and staffing), but a few steps will play a role in success. First of all, the stakeholders across the company need to agree on key performance indicators. The project sponsors will have trouble measuring success and identifying gaps without performance indicators in place. Second, companies should consider pilot testing if possible. Whether focusing on one system companywide such as consolidating and updating distribution logistics software and associated cyber/physical interfaces, or all processes within one facility, both could provide lessons learned for broader rollout. Third, companies should budget time and other resources for developing a baseline for normal operations (for example, a digital twin for a distillation column or data transmission system) so that monitoring protocols have a basis for comparison. Fourth, a company should conduct testing and simulation prior to rollout to make sure the cybersecurity system should work as planned. Last, risk management is an evergreen process: Issues such as governance, effectiveness reporting, and maintenance/update plans should be made to manage ever-evolving threats.

Cybersecurity will become increasingly important to downstream O&G companies, due in part to the sophistication of would-be attackers but mostly to the sheer complexity and scale of digitizing the business. IoT technology and other advanced industry trends hold the promise of increasing efficiency, reducing waste, and transforming entire businesses. However, as the number of sensors, smart algorithms, and automated processes grows, so do the risks. Companies that identify vulnerabilities, build the appropriate analytical frameworks, and take tangible steps forward can face the challenges head-on and reduce cyber risks.

ENDNOTES

1. Andrew Slaughter and Paul Zonneveld, *An integrated approach to combat cyber risk: Securing industrial operations in oil and gas*, Deloitte, May 2017.
2. Ibid.
3. Anshu Mittal, Andrew Slaughter, and Paul Zonneveld, *Protecting the connected barrels*, Deloitte University Press, June 26, 2017.
4. Andrew Slaughter, Gregory Bean, and Anshu Mittal, *Connected barrels: Transforming oil and gas strategies with the Internet of Things*, Deloitte University Press, April 14, 2015.
5. Industrial Control Systems Cyber Emergency Response Team, "*Year in Review*," reports 2010–16, accessed August 10, 2017; Collin Eaton, "*Hacked: Energy industry's controls provide an alluring target for cyberattacks*," *Houston Chronicle*, March 2, 2017.
6. Robert M. Lee, "*Closing the case on the reported 2008 Russian cyberattack on the BTC pipeline*," SANS Industrial Control Systems Security Blog, June 19, 2015.
7. John Gambrell, "*Iran oil industry fires, blasts raise suspicions of hacking*," Associated Press, September 22, 2016.
8. Kim Zetter, "*A cyberattack has caused confirmed physical damage for the second time ever*," *Wired*, January 8, 2015.
9. Based on June 21, 2017, LLS crude oil and Gulf Coast gasoline and low-sulfur, with 3-2-1 crack spread used for approximate operating profitability.
10. US Energy Information Administration, "*Number and capacity of petroleum refineries*," accessed June 22, 2017.
11. Vikram Mahidhar and David Schatsky, *The Internet of Things*, Deloitte University Press, September 4, 2013.
12. Slaughter et al., *Connected barrels*.
13. 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.
14. Slaughter and Zonneveld, *An integrated approach to combat cyber risk*.
15. Ibid.
16. Lalit Shinde, "*Cybersecurity threat detection—the case for automation*," *TechSpective*, September 21, 2016.
17. Geoffrey Cann, "*Have you met my twin? He's digital*," *Digital Oil & Gas*, June 5, 2017.
18. Rodd Seifarth and Carlton Boush, "*Cloud technology boosts oil and gas operations*," *American Oil & Gas Reporter*, March 2013.
19. Derek R. Harp and Bengt Gregory-Brown, "*IT/OT convergence: Bridging the divide*," *SANS*, accessed July 28, 2017.
20. Vernon Irvin, "*3 barriers to cybersecurity success and how to overcome them*," *Forbes*, April 6, 2017.

ABOUT THE AUTHORS

Thomas Shattuck

Thomas Shattuck is a manager with the Deloitte Center for Energy Solutions, analyzing trends in the global energy industry with a focus on LNG as well as petroleum exploration, production, and consumption. Prior to joining Deloitte, Shattuck worked as a market research analyst covering deepwater and frontier oil and gas projects. He also has hands-on experience in the energy industry, working as an engineer for a leading oilfield services company in the Gulf of Mexico.

Andrew Slaughter

Andrew Slaughter is executive director of the Deloitte Center for Energy Solutions. 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 particularly thank **Kushagr Singh**, senior manager, Deloitte & Touche LLP, for his valuable guidance. They also thank: **John England**, vice chairman and US Energy & Resources industry leader, Deloitte LLP; **Suzanna Sanborn**, senior manager, Deloitte Services LP, and **Matthew Budman**, manager, Deloitte Services LP, for their insightful comments and 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

Charles Hosner
Partner, risk advisory
Deloitte UK
+44 20 7007 2827
chosner@deloitte.co.uk

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

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Contributors

Editorial: Matthew Budman and Nikita Garia

Creative: Emily Moreano and Tushar Barman

Promotion: Shraddha Sachdev

Artwork: Infomen

About Deloitte Insights
Deloitte Insights 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 Insights is an imprint of Deloitte Development LLC.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.