bcg.perspectives
by THE BOSTON CONSULTING GROUP

COUNTERING THE THREAT OF CYBERATTACKS IN OIL AND GAS

By Katharina Rick and Karthik Iyer

Across industries, companies have been intesifying their focus on cybersecurity. This is a direct consequence of the expanding role that digitization is playing in their business and operating models and the demonstrated potential for significant damage resulting from a successful cyberattack. Indeed, *CIO* magazine's "2015 State of the CIO" survey revealed that chief information officers now spend roughly a third of their time on cybersecurity-related issues and consider cybersecurity one of their top-four priorities.[1] In our work, we are seeing keen interest in cybersecurity among other senior executives, including board members and CEOs.

Concern about cybersecurity is particularly high at oil and gas companies, which face a far wider spectrum of threats—threats that are potentially more severe—than do companies in most other industries.[2] Transactions in the oil and gas arena are broad in scope—the life cycle of a transaction can include sensitive information on such diverse topics as possible well sites and end-user consumption—so the companies are vulnerable at many different points. These companies are also subject to relatively large-scale threats, given the global nature of oil and gas production and distribution.

Furthermore, the industry faces threats that are activist (including attacks carried out by environmental groups), rather than purely commercial, in nature. These include threats that, if successful, could have severe effects not just on the industry but also on the environment, public health and safety, and even national security.[3]

Recognizing the severity of the situation, many oil and gas companies have taken significant measures to address their vulnerability. Have they done enough?

In a recent survey of a number of industry players, The Boston Consulting Group found, for example, that none of the companies had undergone a comprehensive audit (spanning corporate, upstream, midstream, and downstream operations) of its value chain.

Many Points of Vulnerability—But Where to Focus?

The scope of activities within the oil and gas industry's value chain creates many potential points of entry for attack. (See Exhibit 1.) It also leaves the industry prone to multiple types of attacks. These include attacks on the industry's physical infrastructure (such as cutting fiber-optic cables), the disabling of critical systems (through denial-of-service attacks, for instance), and the theft or corruption of information or the prevention of its dissemination. Given the industry's relatively high degree of automation and interconnectedness, the effects of such attacks could be highly damaging to these companies. These effects can include the loss of equipment (for example, failed pressure-valve systems), the loss of competitive advantage (through the loss of, for instance, confidentiality of production data or possible drilling sites), and even the loss of life.

In light of the industry's multiple points of vulnerability and the potentially catastrophic consequences of a successful attack, it is important to determine where these companies should focus their cybersecurity efforts. An examination of the critical vulnerabilities of analogous industries may be instructive. A 2014 report issued by the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) identified a wide range of information security weaknesses evident across what the US government classifies as "critical infrastructure sectors."[4] The report found that vulnerabilities in three specific realms were most prevalent across these sectors: boundary protection, information flow enforcement, and remote-access control.

Vulnerabilities in these areas can open doors to a range of attacks. Inadequate *boundary protection,* which can make it difficult to detect nefarious activity, can create avenues that allow outside parties to interface with systems and devices that directly support a company's control processes. Mobile and multimedia devices, including smartphones, have become integral parts of what were formerly considered secure boundaries and offer new potential points of attack. Insufficient *control of information flows* can allow attackers to establish unsanctioned and damaging communications using a company's channels, ports, and services. Weak control over *remote access* can create many entry points for unauthorized interfacing with a company's control-system devices and critical components.

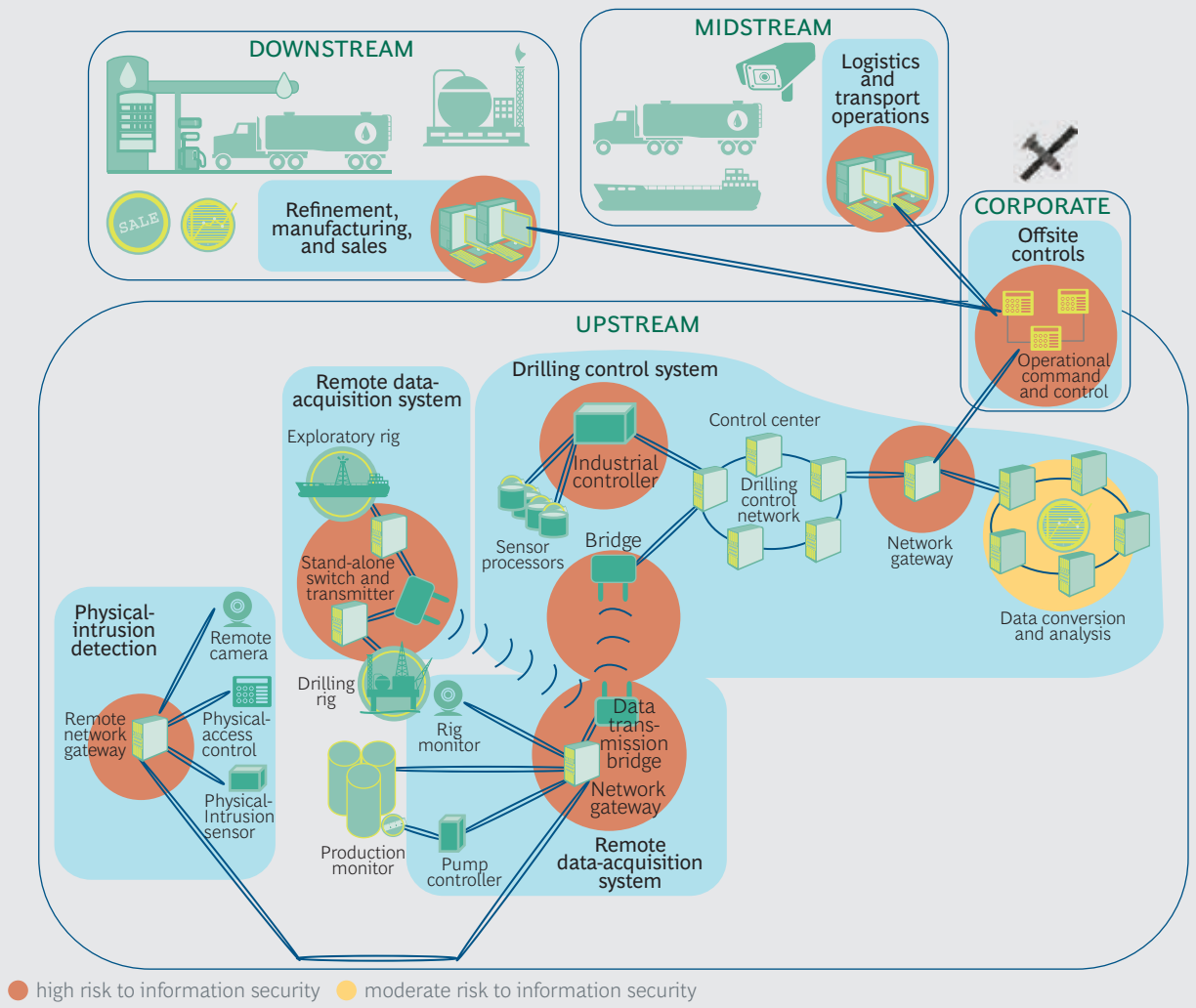
For oil and gas companies, where is the exposure to these three vulnerabilities greatest? To make that determination, we examined these companies' value chains, using the number of systems and integration points as a proxy for exposure. Upstream data emerged as the most vulnerable. We then looked at a simple upstream drilling infrastructure for help in identifying and understanding where the security gaps in upstream operations were largest. (See Exhibit 2.) As the exhibit shows, most security efforts related to upstream drilling infrastructure are focused on the security of physical assets rather than the security of information. Often, for example, data is

Exhibit 1 | Oil and Gas Companies Are Vulnerable to Cyberattacks at Many Points of Entry

CORPORATE DATA	UPSTREAM DATA	MIDSTREAM DATA	DOWNSTREAM DATA
• Production information • Potential partners and acquisition targets • Details on drilling sites • Trading positions • Financial and organizational reports • Capital projects	• Exploratory information • Field production information from sensors • Operational information, for example, on optimal times for reserving a rig, current and future drilling sites, equipment, and personnel	• Supply chain logistics • Distribution network • Storage information • Pipeline and transportation	• Refinery information • Industrial plants and manufacturing • End-user distribution • Retail data • Consumer data

Source: BCG analysis.

EXHIBIT 2 | Upstream Operations Are Particularly Vulnerable



Source: BCG analysis.

transmitted from old or unsecured equipment and without standard protocols or security precautions. As a result, many companies' upstream assets have glaringly unaddressed vulnerabilities to cybersecurity attacks.

Until recently, the industry considered the traditional upstream systems in oil and gas to be relatively safe because they were, in most cases, isolated. But the industry's growing use of connected industrial systems and networking technology—coupled with the ever-increasing need for real-time data and analytics—has introduced new risks. These include asymmetrical threats against which the upstream segment is relatively unprotected compared with the industry's corporate and retail segments. The upstream segment's heavy reliance on oilfield-services companies and use of nonstandard equipment and potentially insecure technologies further increases the number of potential entry points for attack and elevates the risk the segment faces.

To fortify the security of their upstream operations and related information, companies must add a broad and effective security layer on top of their existing upstream defenses. Such a layer, which would allow the companies to proactively detect intrusions and other forms of attack, should consist of such elements as firewalls, network-monitoring equipment, and network use rules that can secure systems

and also enable the infrastructure to detect intrusions and associated patterns. These elements will help ensure that all information flows are authorized and that there are adequate authentication procedures in place to ensure that unauthorized parties cannot gain access to critical systems. This will help oil and gas companies manage cybersecurity risk across the upstream supply chain.

Shoring Up Defenses

Realizing the need for taking concerted action against cybersecurity threats across the entire business, oil and gas companies have taken collective steps to mitigate risks. These include the formation of information-sharing bodies, such as the Oil and Natural Gas Information Sharing and Analysis Center, an industry effort launched in the US in 2014 to provide information and guidance to US energy companies.

Oil and gas companies also stand to benefit from government measures aimed at bolstering their defenses. Many governments, including those of the US, the EU, Russia, and Saudi Arabia, have developed national cybersecurity policies or frameworks, focusing specific attention on critical infrastructure. ICS-CERT, for example, was created to monitor and respond to cybersecurity incidents across critical domestic sectors, performing security assessments of and making recommendations related to industrial systems. The NATO Cooperative Cyber Defence Centre of Excellence seeks to enhance cybersecurity-related capabilities, cooperation, and information sharing among NATO member states, as well as a number of NATO partner organizations from around the world that focus on the issue, including the Euro-Atlantic Partnership Council and the Istanbul Cooperation Initiative.

These various bodies and efforts notwithstanding, individual oil and gas companies need to take primary responsibility for their cybersecurity themselves. (See the sidebar, "An Interview with Risto Siilasmaa and Jens Thonke," for thoughts from two experts on the challenges of building an effective defense.) We recommend a risk-based approach centered on three steps:

- **Develop an understanding of the precise risk to the company's assets and the effort and resources necessary to mitigate them.** With that understanding, the company should prioritize its security efforts. Cybersecurity risk varies considerably, depending on a host of variables, including the type of asset, its position in the value chain, and its physical location. The consequences of an attack can also vary materially. An effective detection and response scheme will aim at addressing the largest threats first.

- **Build and sustain a multilayered defense system.** Such a system should protect against various attack vectors. Management of this is highly complex and requires organizational alignment, the right technologies, clear processes, and strict organizational discipline. Threats to hardware infrastructure, for example, are different from threats to software, and it is imperative that oil and gas companies have resources that address both.[5] Companies must therefore identify vendors whose equipment has been field-tested against a barrage of attacks. The companies must also be able to pinpoint sources of attack and mobilize the right sets of tools and resources in response. The ability to continually monitor all infrastructure, prioritizing threats and defenses, requires both agility and an organizational readiness to redirect technology and people to areas where they are needed most. This system and approach is considerably different from the traditional top-down, linear work-order process that is still employed in many segments of the oil and gas industry.

- **Manage cybersecurity risk on a consistent basis.** The company must be well prepared to detect and respond to various types of attack across the value chain. Reaching this state will demand that the company's processes, systems, and people are continually adapting to

the changing landscape of cybersecurity risk. It will also demand active leadership at the executive level, which is essential for ensuring that the organization is capable of responding to asymmetric attacks quickly and with agility.

These efforts should be supplemented by a number of midlevel priorities, including the following:

- Understand critical assets and the role of information relative to those assets at the institutional level and ensure that the right skills and personnel are available to safeguard vital information.

- Conduct frequent audits and assessments of points at which critical information is being transmitted in order to identify and secure vulnerabilities.

- Engage in data-shaping activities that boost the company's ability to recognize exceptions to normal data flow and transmissions, exceptions that could indicate attempted attacks from external parties.

- Recognize and act on the knowledge that, in many cases, people are a company's weakest links. Most attackers target systems that have been made vulnerable through user apathy, inattentiveness, and ignorance. An organization may have the very best technologies and processes, but if its people are unable or unwilling to comply with established security measures, the effectiveness of its defenses is greatly diminished. Adequate training and awareness is therefore critical for ensuring that the entire organization (including IT staff, R&D professionals, and business and other users)—not just portions of it—is well braced to help resist and weather cybersecurity threats. Active promotion of best practices, such as the use of encrypted storage devices and strong passwords, can go a long way toward creating a robust people defense.

- Ensure that the company's partners—for example, vendors and oil-field-services companies—adhere to the company's organizational-security guidelines, including the use of company-approved hardware and software. Employees of these organizations should also have an adequate understanding of the basic principles of information security and management.

Lower-priority—but still important—measures include ensuring that there is sufficient redundancy in critical systems to enable uninterrupted operations in the event of denial-of-service attacks and providing a "kill switch" to disable connectivity in order to stop an intruder (with sufficient backup in place to allow processes to stop safely). Companies' orientation toward these and all security-related requirements should be comprehensive in nature and focused on continually managing risk, meeting or exceeding industry standards, and limiting negative impact on the business and customers.

The increasing technological complexity of today's oil and gas industry—driven by, for example, the industry's spiraling deployment of data mining and analytics technologies, sensor and networking technologies, industrial systems, and systems integration technologies—is rendering it increasingly vulnerable to cyberattack. To protect themselves, their shareholders, and their customers adequately, industry players must make cybersecurity a highest priority and an ongoing consideration at the executive level.

AN INTERVIEW WITH RISTO SIILASMAA AND JENS THONKE

To broaden our understanding of the current cybersecurity landscape, we recently spoke with Risto Siilasmaa, the chairman, founder, and former CEO of F-Secure, an Internet and cybersecurity software company based in Helsinki, Finland. He was joined by Jens Thonke, executive vice president of cybersecurity services at F-Secure.

Risto and Jens shared insights on a range of related issues. Edited excerpts follow.

The Role of Senior Management

Change starts at the top, meaning with the CEO and board. There is not much knowledge about the technical details of cybersecurity at that level currently. But senior management needs to understand the basics and, even more important, the risks cyberthreats pose to their company.

Gauging the Company's General State of Preparedness

Here's a simple exercise: name the company's three highest-value information assets. These might be the process automation and control system for your production facilities, including Emergency Shut Down systems (ESD) and the oil and gas pipeline solutions; the information system for interacting with suppliers; and the database of customer information, for example. If you can't name the top three, you certainly aren't protecting them sufficiently.

The Necessary Components of a Comprehensive Cybersecurity Program

In our view, there should be four components to a cybersecurity program: intelligence, prevention strategies, detection and recovery, and analysis and learning. *Intelligence* refers to the overall process of staying abreast of relevant information, including vulnerabilities, exploits of attackers, new versions of software, and attacker types and groups. Every company needs to understand how and by whom it is viewed as a target, as well as which of its information assets its potential attackers are after. Oil and gas companies, like other businesses, are attractive to many attackers. These include online criminals who want to cause financial damage and, perhaps, blackmail the company; anonymous attackers who support or claim to support an ideological cause; terrorists who want to cause widespread physical damage (for example, by causing a fire or an explosion); and disgruntled employees, of which—due to industry downsizing—there may now be growing numbers in the oil and gas industry. If you understand who the attackers are and their motivation, you understand what kind of attacks they would likely launch and which of your information assets are most vulnerable.

The second component is *prevention strategies*. Every company has to have its own arsenal of customized approaches to match the variety of potential attacks. The potential damage from an attack can amount to millions, if not billions, of dollars and cost the CEO and other executives their jobs. In a nutshell, it is worth going for best solutions here, not mediocre. The critical goal is to design a holistic and location-independent approach.

The third component is d*etection and recovery*. Companies need to be able to determine when they are under attack and clean up and restore operational capability quickly. They should plan for the inevitable successful attack: given enough time and resources, an attacker will almost always be successful. The sooner a company realizes it is under attack, the sooner it can recover. Recovery is something that companies need to

AN INTERVIEW WITH RISTO SIILASMAA AND JENS THONKE
(continued)

practice, practice, and practice. In terms of types of attack—apart from a physical ruse, such as tailgating or cloning access control cards to trespass in administration offices or command or control rooms—the most common type is a combination of social engineering and customized malware. Systems controls and employees need to learn to be suspicious and recognize such attacks as they are happening. Management should ask basic questions to get a sense of the company's vulnerability. Can anyone gain unauthorized physical access to the company's office or to the executives' e-mail or pretend to be sending messages from their e-mail accounts? Retrieve and modify the source code that runs the company's key products? Access the company's data center?

The final component is *analysis and learning*. Following an attack, the company must work to determine exactly how the attack was carried out; which vulnerabilities in processes, tools, and competencies the attackers exploited; how the company responded to the attack; and how long it took to restore operational capability. The company should then define appropriate countermeasures for warding off future attacks and improving outcomes.

The Challenges That Old or Customized Systems Pose to the Oil and Gas Industry

Many companies are using multiple industrial-control systems, most of which are quite old and proprietary or homemade. Many of them, designed without security precautions in mind, constitute a big risk. A single point could give an attacker an entire system of upstream production assets. For attackers, self-created, older systems are low-hanging fruit.

The Oil and Gas Industry's General Defense Capabilities Relative to Those of Other Industries

The sector's general level of IT security maturity is not that high compared with other industries. In our experience, many companies suffer from a lack of enforcement and control of regulations and policies.

The Emerging Internet of Things and How the Industry's Shortage of Digital Natives Could Hurt It

The Internet of Things could bring a number of new and significant cybersecurity threats to oil and gas companies, and the effects could be compounded by the relatively low share of digital natives among the industry's workforce. Companies with a small concentration of digital natives tend to be less suspicious of attackers' types of activities than are, say, technology companies. Companies with relatively few digital natives also are more apt to create solutions that are not highly secure. Senior management of oil and gas companies should not underestimate the possible challenges of this situation: the backdrop will be increasingly complex as it evolves from the Internet of Things to big data and smart analytics and ultimately to a programmable world.

Notes

1. "2015 State of the CIO," January 5, 2015, http://www.cio.com/article/2862760/cio-role/2015-state-of-the-cio.html#slide9, and Carla Rudder, "These 4 responsibilities just jumped to the top of CIOs' to-do lists," The Enterprisers Project, November 18, 2015, https://enterprisersproject.com/article/2015/11/these-4-responsibilities-just-jumped-top-cios-do-list.

2. Indeed, as oil and gas companies deal with the severe oil-price decline, cybersecurity is among the few areas that they will likely continue to fund.

3. Information on the oil reserves of various nation states, for example, is extremely sensitive, and its illicit distribution could have global geopolitical ramifications. Hence, many governments, as well as businesses, are making concerted efforts to address cybersecurity. See, for example, NATO Cooperative

Cyber Defence Centre of Excellence, "Cyber Security Strategy Documents," https://ccdcoe.org/strategies-policies.html.

4. US Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, *Industrial Control Systems Assessments, FY 2014: Overview and Analysis.* The US Patriot Act of 2001 defines *critical infrastructure* as "…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." According to the US government, there are 16 sectors that fall within this category, including energy, transportation systems, water and wastewater systems, emergency services, dams, critical manufacturing facilities, and chemical facilities.

5. Although companies are inclined to focus significantly on software, the threat of theft or hacking of physical hardware is very real. Use of secure technologies, such as military-grade hard disks and network equipment, can go a long way toward mitigating such threats.

About the Authors

Katharina Rick is a partner and managing director in the San Francisco office of The Boston Consulting Group. You may contact her by e-mail at rick.katharina@bcg.com.

Karthik Iyer is a principal in the firm's Boston office. You may contact him by e-mail at iyer.n.karthik@bcg.com.