Deloitte.

An integrated approach to combat cyber risk

Securing industrial operations in oil and gas

Contents

Foreword

The oil and gas industry is moving into the next stage of evolution, whereby robotics, digitization, and the Internet of Things (IoT) are rapidly being integrated into the operational environment. The interest of cyber criminals in industrial operations has increased over the last decade resulting in cyberattacks that have compromised both production and safety. These attacks have made cyber security a hot discussion topic in boardrooms around the world, and now, a growing number of organizations are developing large transformation programs to address these new operational threats.

However, making operational processes secure, vigilant and resilient is a challenge as this requires the organization to harmonize and align two cultures, engineering and IT. In addition, the operations environment demands tailored technical solutions that are not always easy to secure.

Solving these challenges requires a clear understanding of both the engineering and IT disciplines as well as leading sector-specific cyber security practices. This paper shares the insight gained from our extensive field experience, including lessons learned in helping oil and gas companies to go beyond safety in securing their industrial control systems (ICS). We hope you find this report to be both thought provoking and useful.

Regards,

Paul Zonneveld
Global Energy & Resources
Risk Advisory Leader
Deloitte Canada

This paper shares the insight gained from our extensive field experience, including lessons learned in helping oil and gas companies to go beyond safety in securing their industrial control systems (ICS).

Introduction

Critical infrastructure relies on industrial control systems (ICS) to maintain safe and reliable operations. Engineers have successfully designed and deployed ICS with safety and reliability in mind, but not always security. Why? Originally, there was little need for it. Fit-for-purpose, isolated operational systems were the order of the day. Since these operational systems were not integrated to enterprise systems or even to each other, the risk of a large-scale cascading failure due to an attack, cyber or otherwise, was extremely isolated.

Fast forward 20 years, and the ubiquitous connectivity of the Internet of Things (IoT) has turned the most basic assumptions about operational security upside down. Today, all sorts of industrial facilities, including oil fields, pipelines and refineries, are vulnerable to cyber attacks. Regardless of their location, operational systems can now be compromised by external or internal risks, causing safety or production failures and increasing commercial risk. Although ICS are typically designed to fail safe, the increasing sophistication of cyber criminals heightens the risk of catastrophic incidents, along with the magnitude of the impacts in terms of cost, safety, reputation, and commercial or financial losses.

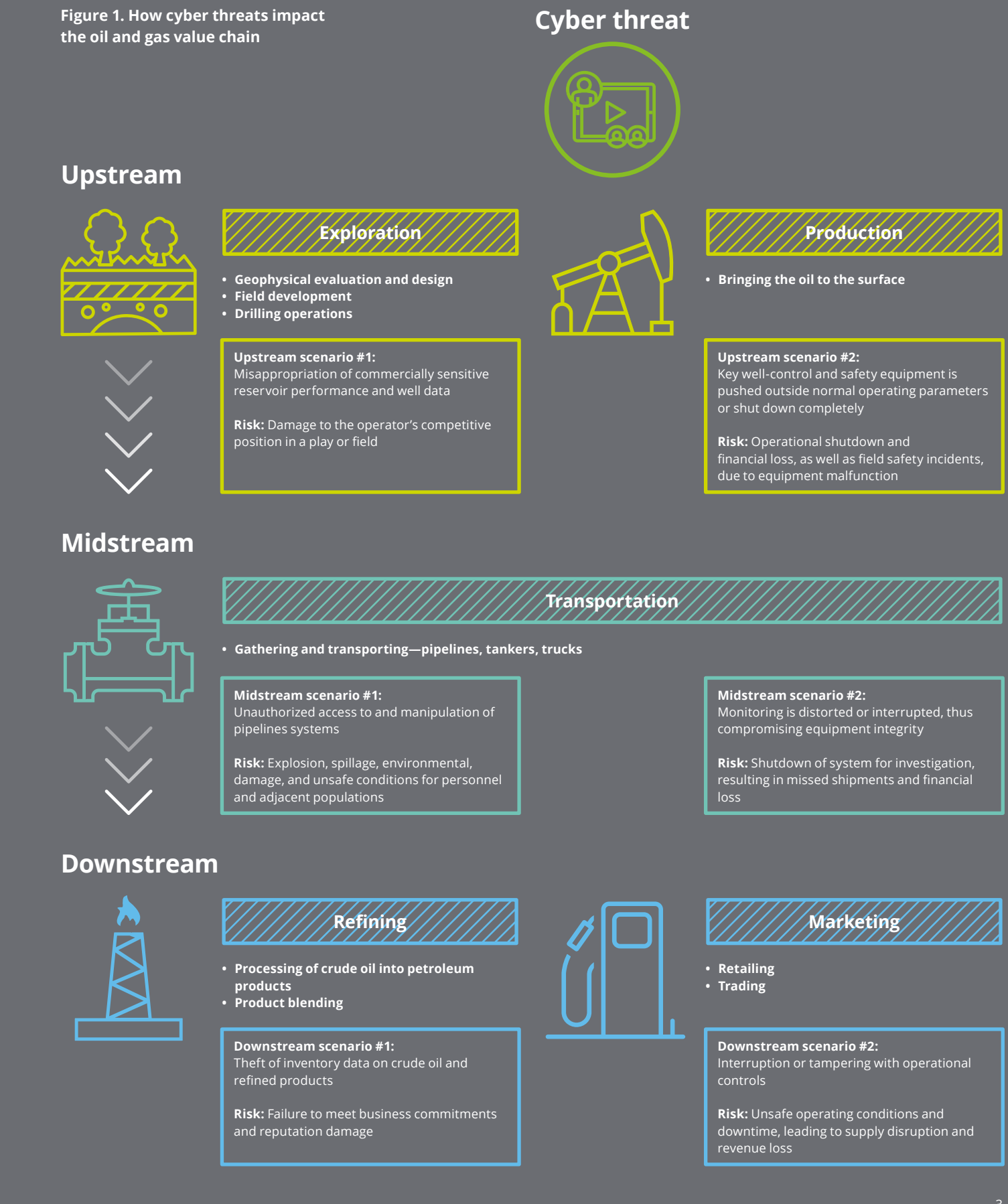
Like other industries, the oil and gas sector has been working to improve cyber security, which is a priority concern among senior leadership and boards of directors.

While the industry has escaped a major operational catastrophe thus far, this good fortune may not last unless companies expand their cyber security programs. To date, oil and gas companies have been primarily focused on protecting corporate, as opposed to operational, systems and data. That's because IoT—where production can be controlled from an iPad or a smart phone, for instance—is relatively new, gaining momentum over the last decade. Also, operational systems are inherently different, requiring engineering know-how, and not just IT expertise, in order to secure them appropriately.

Today, an approach that brings together IT and engineering is needed to address cyber security programmatically and sustainably. The following discusses the goals of such an approach as well as practical steps for getting started. First, let's take a closer look at the types of cyber risks facing the oil and gas industry, how they can disrupt the value chain, and what the consequences could be.

While the industry has escaped a major operational catastrophe thus far, this good fortune may not last unless companies expand their cyber security programs.

Figure 1. How cyber threats impact the oil and gas value chain



Understanding the risks

One of the main factors that makes it so difficult to secure ICS is that they were not designed to be connected; yet, today they are networked. Digitization of operational processes in the oil and gas industry has led to new opportunities to improve productivity and to drive down costs. However, the convergence of operational and business systems has also opened the enterprise to a whole new array of cyber risks. Consider the following scenarios, the possibility of which didn't exist a few years ago:

- Insecure remote access communication allows a cyber criminal to hijack a process control system and push production to unsafe levels.
- Poor security practices by a third-party contractor allow a virus to migrate into the production environment, shutting down critical Supervisory Control and Data Acquisition (SCADA) systems and creating unsafe working conditions.
- Improper testing of IT systems prior to deployment results in a system crash, leading to disruption or shutdown of operations.
- Technology acquired directly by a facility, without adequate testing and evaluation, goes unpatched and introduces a vulnerability which allows members of an adversarial community to gain remote access to programmable logic controllers (PLC), thus giving them the ability to disrupt the production process at will.

As these examples illustrate, cyber threats can come from many directions, including internal actors aiming to sabotage production, competitors seeking to cause brand damage, and external parties, such as activist groups, wanting to shut down operations.

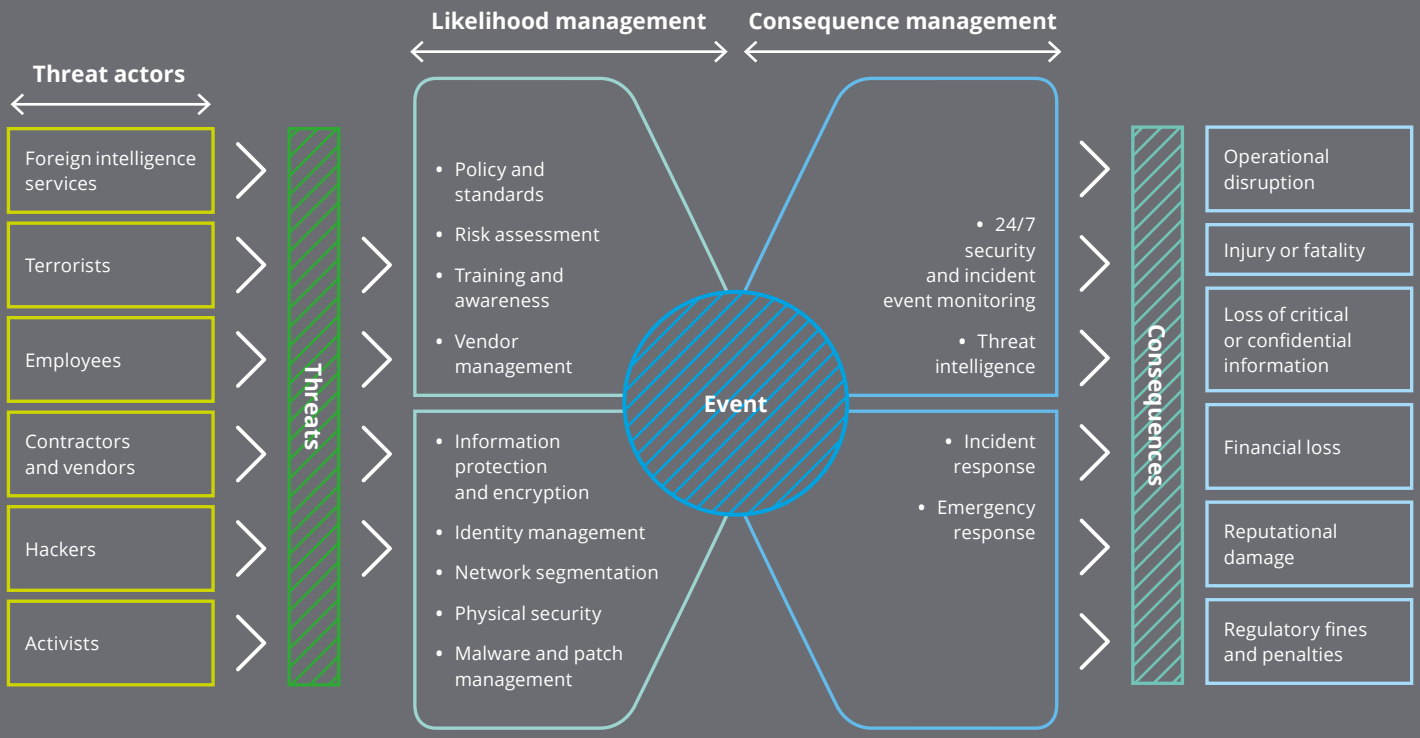
Not all vulnerabilities stem from the technologies themselves; behavioral aspects also come into play. For instance, sometimes a lack of security awareness within the organization can inadvertently expose systems to cyber attacks, such as when employees bring portable media that is infected with malware into the environment. Furthermore, many operations employees simply believe their systems are an unlikely target, thus they are reluctant to buy into the need to change their behaviors and implement new security protocols. After all, not long ago they could safely assume all equipment components were trustworthy, which is no longer the case since digital sensors and controllers can be manipulated to provide false input and misguiding status information. Another outdated assumption is that process failures are mainly caused by weather conditions, human error, and equipment fatigue and not necessarily malicious manipulation of the system by those intending to inflict harm.

Whether a cyber breach is intentional or unintentional, the consequences can be grave, ranging from compromising confidential data to triggering system failure or shutdown. This can result in decreased revenue, reputational damage, environmental disaster, legal penalties, and in extreme cases, loss of life.

It's easy to see why integrating effective and comprehensive cyber security controls into ICS is necessary, if not increasingly becoming mandatory. However, in order to get there, companies must find a way to reconcile the divergent points of view of IT and operations as ICS specialists do not always fully understand modern IT security risks, just as IT security specialists often do not completely comprehend the industrial processes supported by ICS. A bowtie analysis, a common concept used in engineering for failure mode evaluation, can be a useful tool for bridging this gap. While any analysis will be company-specific, figure 2 provides an example of how the bowtie analysis might look for an oil and gas company.

Digitization of operational processes in the oil and gas industry has led to new opportunities to improve productivity and to drive down costs. However, the convergence of operational and business systems has also opened the enterprise to a whole new array of cyber risks.

Figure 2. Example of a "Cyber Risk" bowtie analysis for an oil and gas company



Source: Information adapted from Talbot, J, and Jakeman, M, 2008, 'Security Risk Management Body of Knowledge', RMIA, Carlton South

Conduct a maturity assessment

Once the risks are understood, an oil and gas company should assess the maturity of its cyber security controls in an operational environment. While not every risk can be mitigated, it's important to know what type of controls are in place and where to focus improvement efforts. This means giving appropriate consideration to how potential security breaches within ICS link to business risks. Importantly, this can't be done by an engineering or IT group independently; it requires a multi-disciplinary team of business, operations, engineering, and IT security professionals to:

- **Conduct an inventory assessment of assets and facilities and rank them in terms of criticality**. This can involve asking questions such as: Are there factors that make a certain facility a particularly attractive target? Are corporate IT standards, governance, and monitoring processes being applied to all ICS assets? Have the full range of cyber vulnerabilities been considered, and have the potential consequences been identified and ideally quantified?

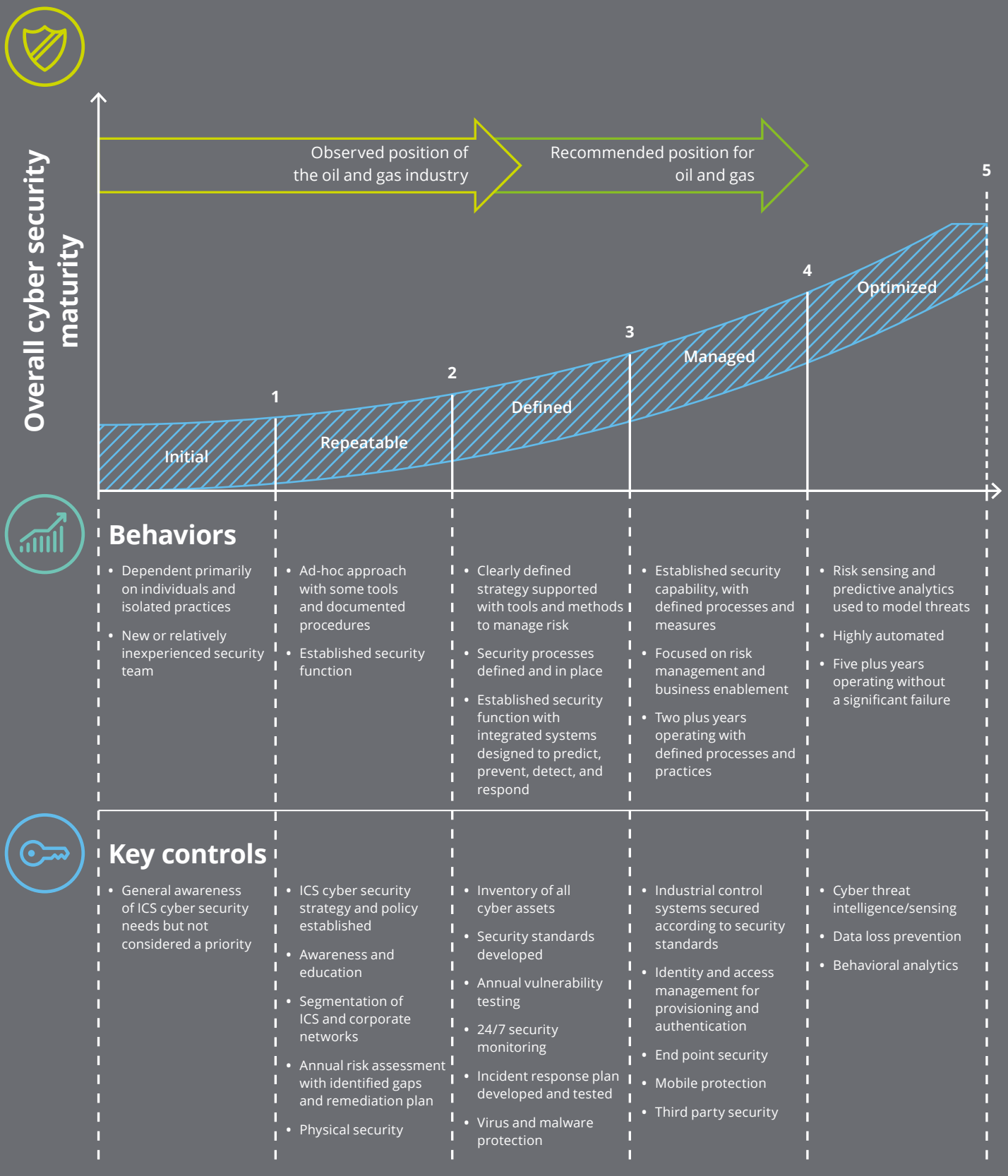
While not every risk can be mitigated, it's important to know what type of controls are in place and where to focus improvement efforts.

- **Determine if critical assets and facilities have well-known and exploitable vulnerabilities**. In the oil and gas industry, these vulnerabilities differ somewhat according to sub-sector. For instance, exploration systems are commonly exposed to theft of proprietary data, such as geophysical surveys, exploration data, well statistics, research studies, and strategic planning information, all of which can jeopardize competitive positioning. Production systems, on the other hand, are vulnerable to manipulation of SCADA and other operational systems, as well as loss of communication to remote facilities and production shutdowns due to virus infections. Here, the consequences are more physical, resulting in unsafe conditions and downtime, which, in turn, could lead to human and financial loss. Similarly, cyber risks in the midstream sector also have both physical and financial implications, such as unsafe conditions, spills, and disruption to delivery or production flow. The downstream sector is also vulnerable to manipulation of operational controls, with the same physical and financial implications as the other sectors. However, downstream also encompasses customer-facing marketing activities, with the potential for theft of customer data and the manipulation of trading systems. This could result in revenue loss, brand damage, and regulatory and compliance violations.
- **Assess the maturity of the controls environment for proactively managing these threats**. In gauging the sophistication of governance and controls, it is often helpful to use an established framework such as the Deloitte cyber security maturity model, which is presented in figure 3. In performing maturity assessments for a broad range of energy and resources companies, we've observed that the maturity of the oil and gas industry as a whole is about 2.5 on this scale, whereas the recommended position is greater than 4.

Throughout the maturity assessment process, it is important to understand the difference between the security considerations for business systems versus industrial control systems. In today's integrated environment, IT security standards and processes must be capable of addressing both back-office systems and ICS in a manner that doesn't interfere with existing mechanisms for protecting safety and reliability.

In addition to the maturity assessment, and as part of ongoing monitoring activities, organization's need to retroactively scour their assets regularly for not only known vulnerabilities but also for emerging threats, advanced persistent threats (APT), suspicious behavior and to identify compromised assets before it becomes an incident.

Figure 3. The Deloitte cyber security maturity model



Build a unified program

For over 50 years, safety was the primary motivation behind designing and deploying controls for physical production processes. While this motivation is still there to keep processes in a safe and operational state, the landscape of potential disruptions now encompasses the cyber domain. This now requires a unified program to address cyber security systematically across the business and operations. Although building and implementing a program of this nature is a multi-year, transformational effort, each phase of the initiative should have the same objective in mind, moving up the maturity scale to create an ICS environment that is secure, resilient, and vigilant.

Secure

Being secure is about preventing system breaches or compromises through effective, automated controls and monitoring. However, it's not feasible to secure everything equally. Critical assets and infrastructure, and their associated ICS, would obviously be at the top of the list, but it's important to remember that they're not isolated components. They're part of larger supply chains; so, it's essential to shore up weaknesses throughout end-to-end processes. This can involve many layers and types of controls, ranging from hardening sensors on processing facilities to installing software firewalls. Systems need to be designed to consider that the entity operating an asset may not be the only organization with rights to data. Service and supply companies and equipment vendors may also be given visibility into operational and equipment performance data in order to improve the services they can offer. Unless properly structured, this might provide an opportunity for unforeseen data leakage or system weaknesses, which could be exploited by third parties. It is essential to build control and monitoring systems with clearly defined data access rights and the ability to identify when these are contravened.

Vigilant

Security alone is not enough. It must be accompanied by vigilance, or continuous monitoring, to determine whether a system is still secure or has been compromised. Worthwhile efforts to be vigilant start with a good idea of what one needs to defend against. There are discernable threat trends in the oil and gas industry, which provide a good starting point for understanding the types of attacks being launched against ICS. These trends, however, need to be supplemented by an understanding of the organization's specific business risks in order to anticipate what might occur and design detection systems accordingly.

Resilient

A resilient organization should ensure it has the plans and procedures in place to identify a cyber attack, contain or neutralize it, and rapidly restore normal operations. We can refer to these steps as detect, respond, and recover, and the protocols for ensuring successful outcomes will depend on the type of cyber issue identified.

At any level of the oil and gas value chain, whether it be upstream wellhead operations, midstream processing plants and pipelines, or downstream refining and delivery logistics, continuous automated monitoring of equipment should allow real-time detection of anomalies. This includes continually knowing the status of pumps, valves, compressors, or process units, including flow rates and patterns of fluids and gasses. Ongoing visibility into these metrics should facilitate rapid reaction to eliminate environmental and safety hazards stemming from out-of-control operations, up to and including shutting down where necessary.

It may be harder to detect the misappropriation or alteration of commercially sensitive data relating to well performance, flow rates, or asset utilization in processing or refining environments. Therefore, it is even more important to build safeguards into the design of these data management systems.

Even if security controls fail and a cyber attack goes undetected, the ability to mount a strong response can help to contain production losses as well as financial, environmental, and brand damage. The response and recovery phases will need to include not only immediate remediation of compromised equipment and systems but also in-depth analysis of where and how cyber attacks occurred, what system vulnerabilities allowed them to happen, and what mitigation measures should be implemented to prevent further risks.

Critically, it's not sufficient to just put playbooks and policies in place. Like a familiar fire drill, they should be rehearsed periodically through cyber war-gaming and simulations that bring together business and technology teams.

Although building and implementing a program of this nature is a multi-year, transformational effort, each phase of the initiative should have the same objective in mind, moving up the maturity scale to create an ICS environment that is secure, resilient, and vigilant.

Implement key controls

While risk appetite and maturity levels will vary, there are a few pillars for cyber risk transformation in an ICS environment that nearly every oil and gas company should have in place. Implementing these key controls can provide a starting point for a customized program aimed at achieving security, vigilance, and resiliency.

- Awareness training: Cyber security awareness needs to be promoted among professionals at different roles in the organization, along with training to give them the necessary skills to interact with systems safely, securely, and responsibly.
- Access control: ICS components, including hardware, applications, and networks, are both physically and logically secured, with access only being granted after formal authentication and authorization.
- Network security: Access to wired and wireless networks within the ICS environment is limited and secured in accordance with leading identity and access management practices, including dynamic provisioning and authentication, 24/7 monitoring, and end point security.
- Portable media: Use of portable media within the ICS environment is restricted and scanned for malicious software.
- Incident response: Incident management policies and procedures are developed and periodically tested.

While risk appetite and maturity levels will vary, there are a few pillars for cyber risk transformation in an ICS environment that nearly every oil and gas company should have in place.

Figure 4: Key controls

GOVERNANCE		SECURE		VIGILANT		RESILIENT	
Cyber Security Management	Rick Management & Compliance	Information Protection	Information Lifecycle Management	Threat Management	Cyber Attack Readiness Testing	Incident Management	Security Incident Response
	Policies & Standards		Encryption	Security Analytics	Security Event Monitoring		Business Continuity Management
	Training & Awareness	Identity & Access Management	Authentication				
	Vendor Management		Roles & Rights Management				
			Identify Lifecycle Management				
		Infrastructure Protection	Network Security				
			Physical Security				
			System Security				
			Patch & Vulnerability				
			Malware Protection				

Embrace good governance

Clear ownership of ICS security is crucial, and roles and responsibilities should be clearly defined for everyone involved, from managers to process operators to third parties. Ultimately, there must be a single line of accountability. Without one, it is challenging not only to define requirements that apply to the whole organization but also to identify where centralized versus local solutions are appropriate.

In the past, the manufacturing and engineering discipline owned the production environment, including ICS and related security mechanisms. Today, ICS security is increasingly becoming a part of the corporate organization, falling under the auspices of the Chief Information Security Officer (CISO). Yet, this isn't about IT stepping in and running the oil field or the refinery. Even with CISO accountability, the engineering organization is still responsible for developing the right solutions and deploying them at the sites.

Implementing a cyber security program within the ICS domain additionally poses some distinct talent management challenges. The job profile often requires people to be stationed at sites for a number of years. Without providing them with a clear career path, two things could happen:

1. IT professionals who are forced into an ICS security role will consider the program as merely a sideline activity and will not actively contribute.

2. Security savvy professionals will quickly reach their peak at a site and then will search for another organization.

Ideally, the organization should develop an awareness program to bridge the gap between IT and ICS professionals, as well as a career development path for those wishing to specialize in ICS security. This path often starts with an entry-level site analyst position and progresses to a global security role within the organization.

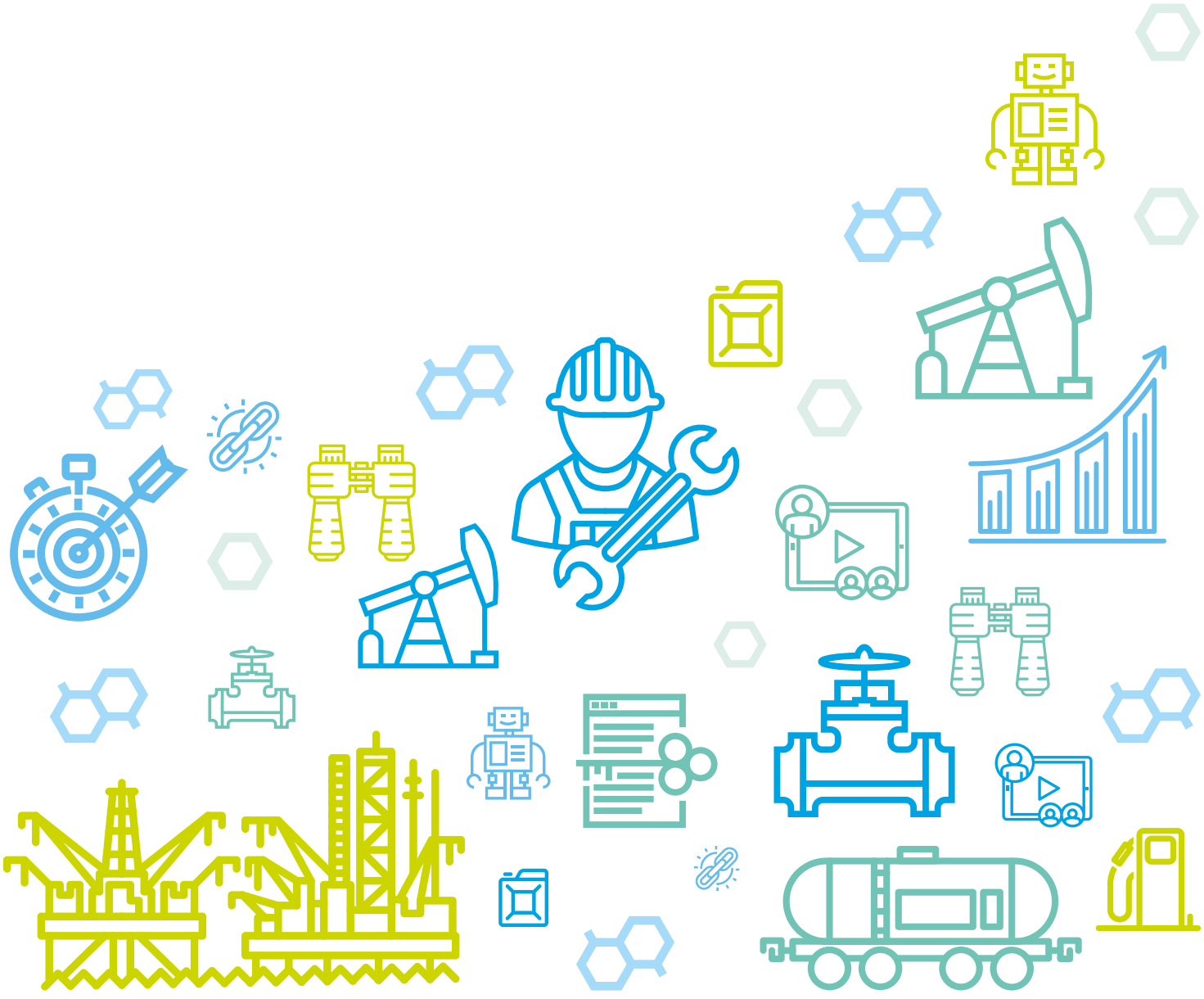
Implementing a cyber security program within the ICS domain additionally poses some distinct talent management challenges.

Conclusion

In the past few years, the oil and gas industry has seen the traditional boundaries between corporate IT and ICS largely disappear. Today, the evolution continues with the digitization of the oil and gas field. As this interconnectedness marches on, so does the frequency and sophistication of cyber attacks. However, most companies have not kept pace in terms of their preparedness.

The place to start is assessing the maturity of the cyber security controls environment. Going beyond traditional operational safety considerations to implement a secure, vigilant, and resilient program is not only essential for enhancing an oil and gas company's ability to protect operational integrity amid a growing range of cyber threats, but also to achieve operational excellence by taking advantage of the productivity benefits offered by a digitized, fully integrated ICS environment.

The call to bridge the cyber-readiness gap has never been louder, with growing public awareness of cyber crime and the potentially disastrous impact it can have on critical infrastructure.



Contact us

Deloitte can assist you in conducting a cyber security maturity assessment.
For more information, contact one of our risk management professionals below:

Authors

Paul Zonneveld
Global Energy & Resources
– Risk Advisory Leader
Deloitte Canada
+1 403 503 1356
pzonneveld@deloitte.ca

Andrew Slaughter
Executive Director
– Deloitte Center for Energy Solutions
Deloitte US
+1 713 982 3526
anslaughter@deloitte.com

Global contacts

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

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

Paul Zonneveld
Global Energy & Resources
– Risk Advisory Leader
Deloitte Canada
+1 403 503 1356
pzonneveld@deloitte.ca

Steve Livingston
National Power & Utilities
– Risk Advisory Leader
Deloitte US
+1 206 716 7539
slivingston@deloitte.com

Dina Kamal
National Energy & Resources
– Risk Advisory Leader
Deloitte Canada
+1 416 775 7414
dkamal@deloitte.ca

Ramsey Hajj
Risk Advisory
– Senior Manager
Deloitte US
+1 561 962 7843
rhajj@deloitte.com

Amir Belkhelladi
Risk Advisory – Partner
Deloitte Canada
+1 514 393 7035
abelkhelladi@deloitte.ca

Marko Van Zwam
Risk Advisory – Partner
Deloitte Netherlands
+31 88 288 0890
MvanZwam@deloitte.nl

Tiaan van Schalkwyk
Risk Advisory – Associate Director
Deloitte Africa
+27 11 806 5167
tvanschalkwyk@deloitte.co.za

Charles Hosner
Risk Advisory – Partner
Deloitte UK
+44 20 7007 2827
chosner@deloitte.co.uk

Rob Hayes
Risk Advisory – Director
Deloitte UK
+44 20 7007 2606
rjhayes@deloitte.co.uk

Deloitte.

Designed and produced by The Creative Studio at Deloitte, London. J11747