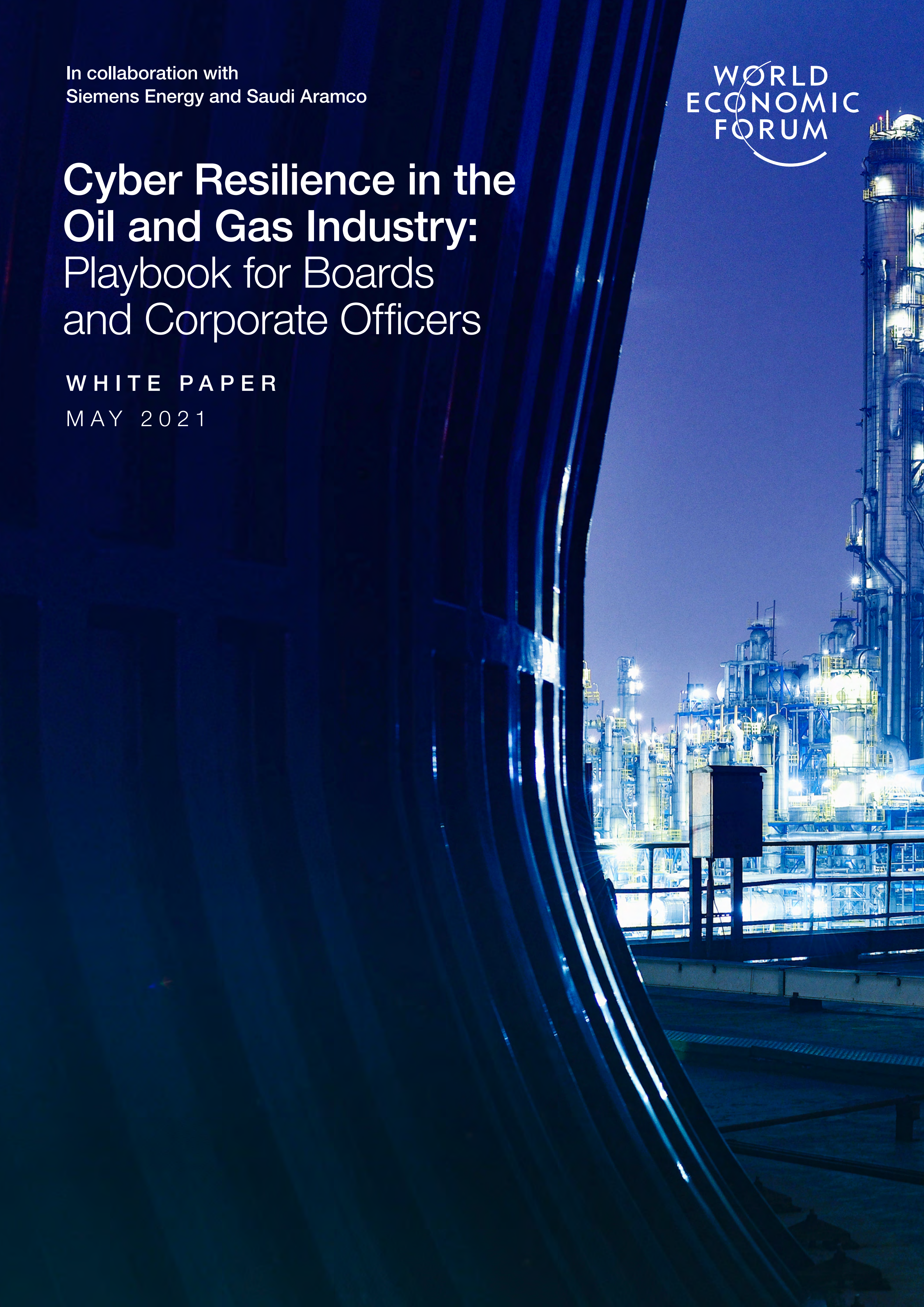
In collaboration with
Siemens Energy and Saudi Aramco

WORLD
ECONOMIC
FORUM

Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers

WHITE PAPER

MAY 2021



Cover: Zora Zhuang, Getty Images – **Inside:** Getty Images, Unsplash

Contents

Foreword

Leo Simonovich
Vice-President and Global Head, Industrial Cyber and Digital Security, Siemens Corporation, USA

Basim Al-Ruwaii
Chief Information Security Officer, Saudi Aramco, Saudi Arabia

Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum

The digital revolution and the energy transition have jointly transformed the oil and gas industry's decades-old business model in just a few short years. Today, companies control physical energy assets by linking operational technology with information technology networks that leverage big data, artificial intelligence and automation. These new, pervasive linkages serve as the lynchpin to a more efficient, resilient and lower-carbon operating model for the energy sector.

As one of the world's most sophisticated and complex industries makes a multifaceted transition – from analogue to digital, centralized to distributed and fossil-based to low-carbon – managing cyber risk and preventing cyberthreats are quickly becoming critical to company value chains. Executive board members, corporate leaders and cybersecurity managers must evaluate and ensure cyber risk is addressed in all aspects of their business – from connected physical assets deployed in remote field environments to business software used in corporate headquarters in some of the largest cities in the world.

To stay ahead of cyberattacks, vulnerabilities and insider threats in this rapidly evolving industry, oil and gas companies must make sure cyber-risk mitigation progresses at the same pace as innovation. This means executives must continually improve their organization's cyber resiliency, evaluate new and existing risks, and create a dialogue between board members, corporate officers and key security professionals. To help the energy industry advance this crucial task, the World Economic Forum has convened a group of more than 40 senior executives from the oil and gas industry with the goal of establishing a blueprint for evaluating cyber risk and enhancing cyber resilience across the industry.

This publication, *Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers*, is the result of community members leading in-depth discussions to illuminate the industry's best practices and create new solutions that help corporate leaders address cyber risk. We encourage community members and other companies in the oil and gas ecosystem to adopt these principles and pledge their commitment to addressing cyber risk so the industry can continue to meet customer needs and deliver safe, affordable and low-carbon energy for decades to come.

Executive summary

The oil and gas sector's future relies on digitalization to manage a vast network of global energy assets and operations to maximize profits, improve safety and efficiency, and minimize emissions in the midst of a volatile market. The new wave of digital solutions integrates operational technology (OT) and information technology (IT), leveraging the power of emerging technologies (e.g. automation and artificial intelligence), to help the oil and gas industry innovate for the energy transition. This shift exposes critical infrastructure and entire supply chains to cyber risks, making cybersecurity a core requirement of the business model.

Within this integrated digital ecosystem, it is now the responsibility of the corporate leadership to take cyber risk into account when assessing stability and security. Not only must the leadership manage cyber risks at the executive level, but these leaders must also ensure that cyber risk is a core aspect of the operational and corporate culture – starting at the top, and cascading and implementing clear policies across vast, global organizations.

To effectively manage risk in this new operating environment, boards need the tools to ensure their organizations develop and maintain appropriate cyber-resilience measures. Leading executives must build cyber resilience and collective defence systems across the industry that uphold common standards and protect partner supply chains, and collaborate on risk-based approaches to ensure the oil and gas sector's overall security.

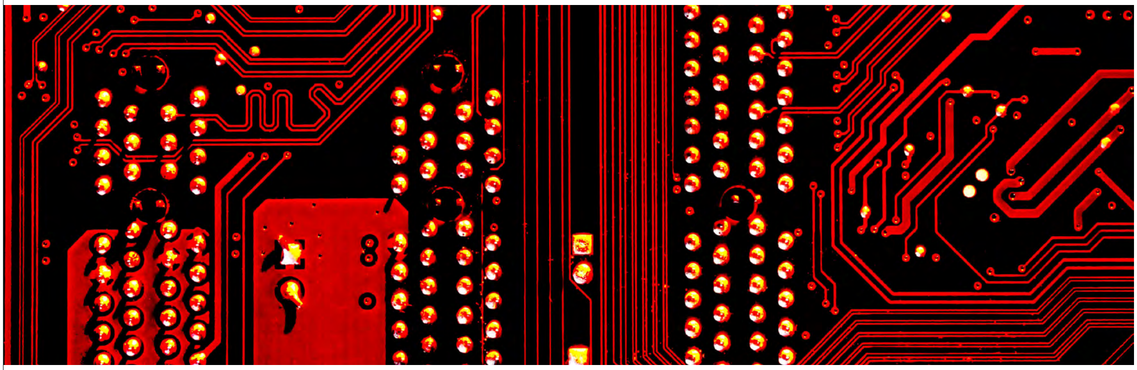
This playbook for boards and corporate officers provides guidance to those responsible for implementing cyber resilience to improve the industry's readiness to mitigate cyber risks.

1 Introduction

Cybersecurity failure, including cyberthreats and vulnerabilities, are identified as a top short-term (0-2 years) business challenge for most organizations in the World Economic Forum *Global Risks Report 2021*.[1] To address cyber risk across the oil and gas industry, board managers and senior corporate leaders must act to secure industrial operating environments from the increasing threat of cyberattacks with new policies, processes and attention from corporate officers. Today, board members must balance the competitive advantage associated with digitizing their company's industrial operating environment with greater exposure to malicious cyberthreats seeking to disrupt operations for financial gain or other nefarious motivations, such as geopolitical conflict or terrorism.

To overcome market pressures, adapt to the energy transition and succeed in this new operating environment, the industry's future increasingly depends on digitally connected OT to control physical energy assets – such as gas compressors and offshore drilling equipment – with IT applications to optimize data that turns a company's operations into an interconnected network. Board-level executives, corporate managers and industry stakeholders view the widespread use of digital technologies to run, manage and collect data from physical energy assets and plant operations as the key enabler to reduce costs, improve efficiency and reduce emissions.

As the oil and gas industry's digital transformation exposes all aspects of its businesses to increased cyber risks, the companies become increasingly more vulnerable to widespread cyberthreats.[2] Cybersecurity becomes even more difficult to ensure in an expanding digital threat landscape and complex global industrial environment.



The oil and gas sector's expanding digital threat landscape

With industrial device connections expected to reach 37 billion by 2025,[3] digitalization is rapidly transforming the oil and gas industry from a commodity-based business run on analogue equipment into an automated, remotely controlled and artificial intelligence (AI)-driven industry that makes risk-based decisions with internet-like speed. This rapid pace of digitalization comes at a cost, however; as oil and gas companies digitize operations, they simultaneously expose their companies to cyber risks.

Malicious actors increasingly view the energy industry as a ripe target to launch cyberattacks for financial, criminal or geopolitical gain. Recent studies show the volume of attacks against OT-connected assets increased over 20 times from 2018 to 2019.[4] Meanwhile, the average energy-sector data-breach cost has risen more than 13% since 2019, to $6.39 million – a higher cost than the global average of $3.86 million.[5] Yet, even with expanding cyberattacks threatening the industry, two-thirds of oil and gas executives state that digitization is benefiting their business and will remain essential for their company's success.[6]

As companies decide that continuing to incorporate digital technologies across their enterprises outweighs the increased risk of cyberattacks, they should make cybersecurity a core competency of their organization and place it at the centre of the future oil and gas business model. Yet, most oil and gas companies are not accustomed to thinking of themselves as digital companies and therefore lack the cybersecurity technologies, systems, personnel and protocols to protect industrial operating environments.

The complexities of securing global industrial operating environments

Cybersecurity in the oil and gas sector is inherently challenging due to the complexity of running a vast organization with different businesses, assets and personnel located all over the world, as well as working with a complex supply chain of customers and suppliers. Without robust cybersecurity technologies and protocols, companies slow to prioritize the deployment of monitoring and defence solutions for vulnerable devices as well as proper cyber hygiene will find themselves unable to compete with cyber-protected peers offering products and services that are reliably and efficiently delivered.

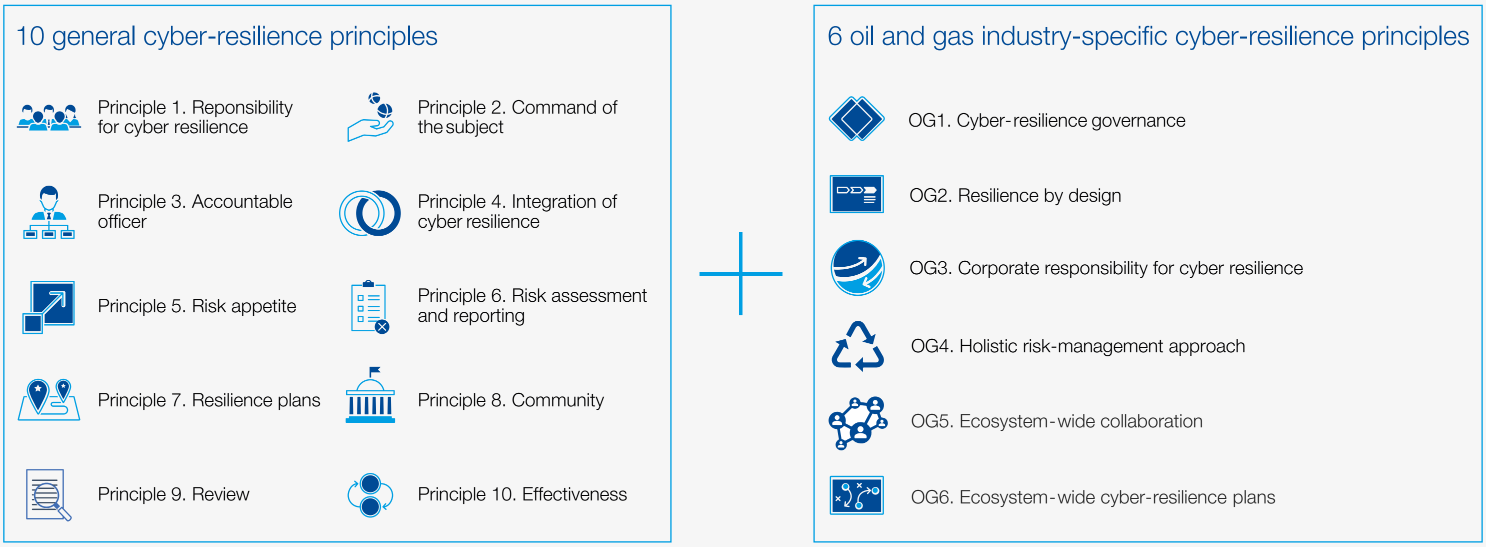
The industry's key cyber challenges in a global operating environment

In many cases, companies face challenges with internal cyber hygiene as systems are interconnected but responsibility is siloed or shared across many partners with diverse priorities. Companies also face challenges with aligning IT and OT departments, managing interoperability with proprietary technologies and engaging with trusted third parties so that every connected device – from wellhead to corporate computer – is protected. While this continuity is necessary to achieve an ecosystem-wide cybersecurity approach, it is difficult to execute.

Many organizations find cybersecurity's complexity overwhelming, and this is particularly true when needing to secure both OT and IT environments. Companies with deeply integrated OT and IT assets need strategies to proactively manage risk today and mature cybersecurity with an eye towards their future risk environment.

This document sets out six principles to help boards at oil and gas companies mature their approach to cybersecurity (Figure 1). They are designed to guide board members through the process of cultivating a corporate culture that assesses and manages cyber risk. Ten broad cyber-resilience principles developed by the World Economic Forum that can be applied to any organization supplement this knowledge (see Appendix A).

FIGURE 1 Cyber resilience principles for the oil and gas industry



10 general cyber-resilience principles

Principle 1. Reponsibility for cyber resilience

Principle 2. Command of the subject

Principle 3. Accountable officer

Principle 4. Integration of cyber resilience

Principle 5. Risk appetite

Principle 6. Risk assessment and reporting

Principle 7. Resilience plans

Principle 8. Community

Principle 9. Review

Principle 10. Effectiveness

+

6 oil and gas industry-specific cyber-resilience principles

OG1. Cyber-resilience governance

OG2. Resilience by design

OG3. Corporate responsibility for cyber resilience

OG4. Holistic risk-management approach

OG5. Ecosystem-wide collaboration

OG6. Ecosystem-wide cyber-resilience plans

Source: World Economic Forum

CASE STUDY

The importance of operational technology to guard against cyberattacks (an experience from Dragos)

Scenario: From 2014 to 2017, a malicious adversary breached the cyber defences of an oil and gas refinery using OT specific malware called Trisis or Triton to target the safety systems used for oil and gas production.

After going undetected for three years by the oil and gas company's security team, the attackers activated their malware to disrupt the refinery's safety instrumented systems. But when the attack was deployed in the summer of 2017, an error in the malware caused the plant to shut down instead of causing significant physical damage and killing or severely injuring company workers as intended. Little did investigators know at the time that this failed attack was the first known cyberattack specifically aiming to kill people.

Immediately following the attack, plant security personnel – and their third parties – did not consider the sudden shutdown to be a direct result of a cyberattack and, thus, did not investigate this possibility as a root cause in their analysis. Years of investing in IT security but without taking a specific approach to OT cyber protection left the organization unprepared to deal with the attack or conduct the investigation. Having failed to correctly recognize and block the ongoing cyber-breach threat, the plant went back into operation with the malicious actor still present.

With the malware still active, a month later attackers made a second attempt to disrupt the refinery's safety system, but this time attempted to shut down even more critical infrastructure; fortunately, the attackers again failed due to a different error. This time the plant's security team requested support from OT specialists to investigate the shutdowns in greater depth. After the second investigation, security experts found that the plan's OT systems were being manipulated. They discovered that attackers were maliciously manipulating OT network activity and took steps to secure the breach. Recovering from the incident and then restoring the refinery to full operation took over 70 days and cost tens of millions of dollars. This attack could have been detected with an OT-specific approach and with a rehearsed incident-response plan in place. Had these measures been deployed, the time lost and the impact of the OT-specific attack would have been significantly reduced.

Key takeaways: Adversary errors prevented casualties in this incident, but board governance can – and should – make organizations more resilient against OT cyberthreats to critical safety infrastructure by taking an OT-specific approach to cybersecurity where appropriate. Attacks will happen as they cannot all be prevented, but organizations can also detect and respond, making themselves more resilient. After incidents, sharing information and lessons learned from past threats helps other organizations in the oil and gas value chain prepare.

The six principles above will help businesses in incidents like this consider how they could apply them to increase their cybersecurity awareness and advance the overall level of cybersecurity at the company.

2 How to use this playbook

This playbook outlines six principles for the oil and gas industry that will help board directors govern cyber risk. It provides guidance for corporate officers and other leaders to strengthen their organization's cybersecurity posture and ensure broader ecosystem cyber resilience.

Are you a board member?

Boards of directors are the ultimate entity accountable for the safety and security of a company's financial, legal, strategic and ethical decisions. Increasingly, executive board members are focusing on new and emerging digital technology issues that threaten the resilience of their organization's operations. In today's digitally connected global economy, cybersecurity is a complex and critical discipline in itself; it requires meticulous technical and operational oversight to keep pace with ever-evolving cyber risks and threats.

This playbook provides board members with guidance to help execute their oversight role and obtain actionable insights to improve cyber resilience.

Are you a corporate officer or manager responsible for cyber resilience?

Corporate officers and managers responsible for cyber resilience must clearly explain to boards why cyber resilience matters for the current and future security, and success, of their organization. They must also be able to articulate their strategy for managing cyber risks.

The corporate officer or manager responsible for cyber resilience is often a senior executive with essential cybersecurity responsibilities, including overseeing a cyber-resilience strategy and reporting to – and advising – a board of directors on the cyber risks facing a company. In many organizations, this role is called the chief information security officer (CISO). This title emphasizes the responsibility and accountability that this individual holds within an organization, regardless of the specific job title.

This playbook provides corporate officers and managers with recommended activities to help implement cyber-resilience principles and facilitate communication on the risks with executive board members.

3 Cyber-resilience principles for oil and gas industry boards

The following six principles are specific to the oil and gas (OG) industry and complement the general cyber-resilience principles[7] to address vital cyber-resilience challenges.[8,9] These principles are designed to enable board action in advancing systemic cyber resilience.

3.1 Principle OG1 - Cyber-resilience governance

The board should require management to establish a comprehensive cybersecurity governance model. This includes oversight into IT, OT, physical security, health and safety environment, and digital transformation to ensure interoperability within the organization and drive alignment across the ecosystem.

Boards acting on cyber resilience should consider the following questions:

- How does the governance model create a collaborative relationship between IT, OT and physical security functions? What effective mechanisms are in place for this?
- Which roles and responsibilities for cyber resilience have been established, integrated and adhered to across IT, OT and physical security functions?
- What are the existing incentives for best practices to secure operational and safety environments?
- How is the cyber-resilience governance model reviewed? How is alignment with the evolving ecosystem and associated cyber risks ensured?

CASE STUDY

Saudi Aramco sets oversight

Scenario: Saudi Aramco took proactive measures to establish a new organizational structure and engage personnel to address cybersecurity oversight and implementation for IT and OT.

Saudi Aramco decided that the best way to defend the organization was with a proactive and risk-based strategy and a dedicated structure to improve cyber hygiene and governance. As a crucial early step, the company appointed a CISO to institute cybersecurity governance and oversee the enterprise's cybersecurity posture, including IT and OT. The CISO helped ensure security and the resilience of connected physical assets and technology devices that could be vulnerable to attack.

The company established a risk-based cybersecurity programme and strategy to cover cyber resilience, and aligned its structure to meet industry frameworks and standards, like the US National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and the Cybersecurity Capability Maturity Model (C2M2). A new oversight mechanism was put in place with the board of directors overseeing top corporate cyber risks and executive management overseeing cybersecurity performance through designated key performance indicators. This approach was designed to support managers and executives in making informed decisions in alignment with pre-set risk tolerance and appetite.

Key takeaway: New personnel, protocols, oversight structures and periodic reporting to the board and executive leadership helped to gain stakeholder buy-in as well as increase cybersecurity awareness and the overall level of cybersecurity at the company.

3.2 Principle OG2 - Resilience by design

The board should promote a *security by design, resilience by design* culture, and should require its management to implement similar standards and values while documenting progress.

Boards acting on cyber resilience should consider the following questions:

Are cyber risks and associated implications evaluated, embedded and appropriately managed in all aspects of the business by design?

How is cross-functional and cross-departmental ownership of cyber-risk management established to achieve resilience by design?

How are cyber risks and their cascading effects managed in ongoing activities and planned for new initiatives?

How are key members of personnel made aware of the cyber-resilience impacts and expectations of their role?

CASE STUDY

Ecopetrol integrates cybersecurity risk

Scenario: At petroleum company Ecopetrol, taking cybersecurity seriously means that it should be integrated throughout all aspects of the value chain, from IT devices to energy assets connected by OT control systems.

This overarching principle has been cascaded throughout the company's approach to integrate cyber-risk management at all points in its operations. To enforce the importance of cyber risk, board members and the CEO developed and endorsed key cyber principles in a memorandum that was communicated to the company by the chief operating officer and chief information officer.

The memo's central goal was to integrate cyber into all the enterprise's operational tasks, beginning with IT and OT environments, as well as in all the processes in business units and holding companies. With the board leading oversight and the implementation of key guidelines, Ecopetrol prioritized cyber risks linked to the strategic risks.

Key takeaway: With board support, the team was able to strengthen its cybersecurity programme by adding personnel and funding and establishing a "Cybersecurity Governance System" to better manage these risks.

3.3 Principle OG3 - Corporate responsibility for cyber resilience

The board should encourage management to consider cyber risks to the organization and the broader ecosystem, examine the organization's cyber culture and practices, and explore how to manage these risks.

Boards acting on cyber resilience should consider the following questions:

- How does management view the cyber-related risks that the organization is introducing to the ecosystem, the potential cascading impact and corresponding reputational risk?
- How are the primary and cascading effects of cyber risks evaluated and managed in all aspects of the business, and how are the potential cascading impact and corresponding reputational risk assessed?
- How does the organization plan to communicate a potential cyber risk, vulnerability and incident introduced to the ecosystem to relevant parties?

CASE STUDY

Repsol shifts from cybersecurity to cyber resilience

Scenario: Many organizations harbour different cultures with various risk appetite levels, which can be detrimental to implementing company-wide cybersecurity policies and best practices. With the goal of reducing the potential impact of cyberattacks at Repsol, the CISO recognized the need to balance risk appetite levels within business units with stakeholder expectations in order to implement cyber resilience holistically throughout the company.

Using the World Economic Forum's principles for boards while building a trusted relationship with board members, the CISO shifted the company's cybersecurity strategic plan from a technical-solutions approach to a business-resilience and risk-management approach. The board provided support for training and awareness as well as resources dedicated to developing Repsol's cyber resilience further. The CISO was able to provide budget support to other departments for lighthouse projects on cyber resilience.

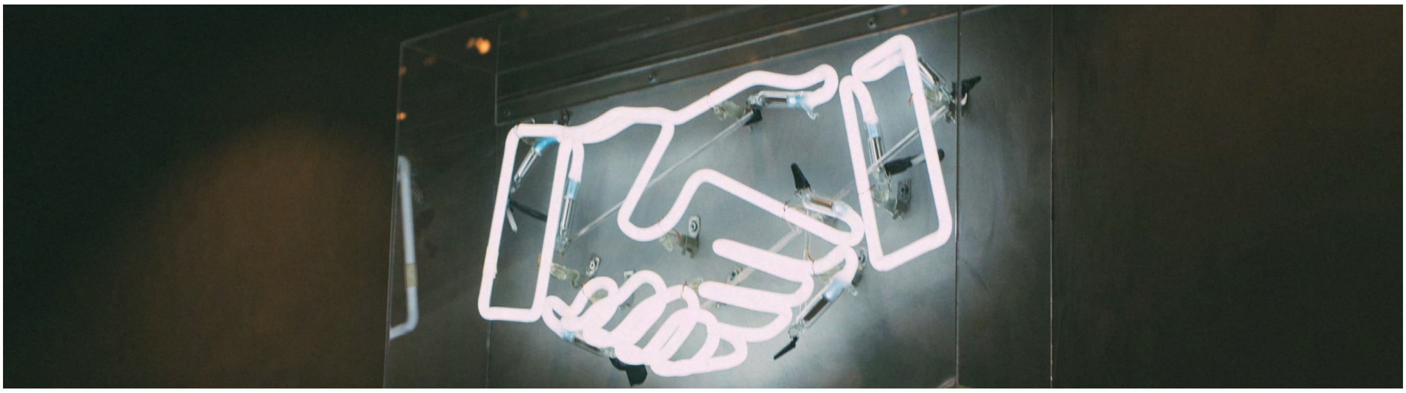
Key takeaway: By ensuring the CISO had the appropriate resources, the board provided the means to build allies in implementing new cyber policies and practices.

3.4 Principle OG4 - Holistic risk-management approach

The board should ensure that cyber risks are managed and mitigated across the oil and gas ecosystem by providing an adequate mandate, funds, resources and accountability for cyber-resilience programmes and reporting.

Boards acting on cyber resilience should consider the following questions:

- What risks for the organization do internal and external parties pose?
- What financial and personnel resources are adequate to achieve the appropriate holistic cybersecurity risk-management objectives?
- How does the current risk-management approach incorporate cyber risks from the supply chain?
- How does the organization manage unknown cyber risks?



3.5 Principle OG5 - Ecosystem-wide collaboration

The board should encourage and empower its management team to create a culture of collaboration for the effective oversight, monitoring and control of ecosystem-wide risks.

Boards acting on cyber resilience should consider the following questions:

- How does the organization engage with cyber-resilience collaboration platforms and action groups?
- What cyber-resilience plan of action covers the organization's ecosystem(s)?
- How are the lessons learned from collaboration activities used to strengthen the organization's and ecosystem's cyber-resilience practices and how are they enabling new opportunities?

CASE STUDY

Establishing an ecosystem-wide approach at Suncor

Scenario: Energy company Suncor's dispersed ecosystem relies on different organizations, partnerships and joint ventures throughout its upstream to downstream business. Each brings its own operating environmental norms and diverse approaches to cybersecurity, which can prove challenging when cyber-related incidents occur.

To reduce cyber risk, Suncor launched a pilot initiative aimed at bridging the gap between these different operating environments and connecting the OT upstream and downstream teams together. During the pilot phase, the centralized team is being financed by the IT group to ensure common practices and approaches to cyber risk, a standard infrastructure and consistent asset inventory tools, and aligned processes to continuously monitor the OT environment. Through this centralized team, Suncor can continuously improve the collective cyber-resilience controls and plans between upstream and downstream partner organizations. This methodology balances preparedness and protection while improving monitoring and response capabilities.

Key takeaway: Collaborating and aligning on the adoption of unified approaches and controls improved the monitoring and visibility of the OT environment, reducing the detection and response time of IT/OT software versioning and patching from a few days to minutes.

3.6 Principle OG6 - Ecosystem-wide cyber-resilience plans

The board should encourage management to create, implement, test and improve collective cyber-resilience plans and controls with other members of the ecosystem. These plans should consider preparedness and protection (e.g. defence in depth strategies[10]) in conjunction with response and recovery capabilities.

Boards acting on cyber resilience should consider the following questions:

- What activities are included in the cyber-resilience plan? How does it cover the organization's ecosystem(s), including incident response, communications, business continuity and disaster recovery? Is it adequately tested with appropriate regularity?
- Which collaboration platforms should boards and management teams support to advocate for the development of collective resilience plans?
- How do the collective resilience plans reflect and balance preparedness with response and recovery across the ecosystem?

CASE STUDY

Siemens Energy helps secure weak links in the value chain

Scenario: In 2019, Siemens Energy and the Ponemon Institute collaborated on a survey[11] of industry executives and managers at global oil and gas companies to assess the companies' cybersecurity readiness. The results of the survey showed that, across the sector, most organizations have difficulty hiring cybersecurity personnel with in-depth knowledge of OT-connected energy assets necessary to identify and address cyberattacks before they occur. Additionally, only the largest organizations were able to fully fund research and development in new technologies and procedures that would improve cyber readiness against an expanding attack environment.

Siemens Energy recognized that one way to improve cybersecurity for all oil and gas companies is to ensure small and medium-sized organizations can access advanced AI-based monitoring and detection solutions, which would help strengthen the weaker links against cyberattacks in the digital ecosystem. In 2020, Siemens Energy developed an AI-based, OT-native cybersecurity solution aimed at solving the technical and economic challenges associated with expanding monitoring and security that all organizations could access.

Key takeaway: By combining interoperable and manufacturer-agnostic AI technologies, and efficiently leveraging OT-native human expertise, small and medium-sized energy companies can gain access to monitoring, detection and cyberattack prevention capabilities – a level of protection only previously achieved in-house at companies with ample budgets.

4 Implementing the oil and gas principles

The cyber-resilience principles for oil and gas industry-specific activities provide cybersecurity practitioners with implementation support. The aim of this guidance is to help corporate officers and managers responsible for cyber resilience to implement these principles and assist board members in exercising their oversight responsibilities.

4.1 Principle OG1 – Cyber-resilience governance

The board should require management to establish a comprehensive cybersecurity governance model. This includes oversight into IT, OT, physical security, health and safety environment, and digital transformation to ensure interoperability within the organization and drive alignment across the ecosystem.

Suggested activities for the implementation of cyber-resilience governance include to:

- Build a comprehensive governance model with the capacity to manage and oversee cyber resilience for IT, OT, physical security, health and safety environment, and digital transformation
- Ensure the proper level of authority and command of accountable officers and subject-matter experts, with the experience and resources to fulfil cybersecurity duties
- Provide regular updates in close collaboration with different business unit leaders at an adequate frequency for cyber-resilience strategy implementation and budget
- Promote a cyber-resilience culture by communicating best practices regularly through training and awareness exercises across the organization
- Establish clear, practical and comprehensive cyber-resilience policies, standards and guidelines throughout the organization, including for IT, OT and IoT environments and third-party business suppliers and ecosystem partners.

Suggested metrics can include the:

- Percentage of employees who have successfully completed cybersecurity awareness education programmes on cyber-hygiene practices with a focus on high-risk groups (e.g. board members, C-suite executives, and IT, engineering, human resource and finance personnel)
- Number of cybersecurity collaborative engagements with business units
- Identification of critical actions during cybersecurity and audit reviews, including the completion rate and the number of actions that remain outstanding; this can include actions relating to executive management accountability and responsibility.

CASE STUDY

Cybersecurity as a business enabler

Scenario: In 2020, oil and gas company Eni reorganized and adopted a new organizational model to achieve significant decarbonization goals, with technological innovation and digitalization as the strategic drivers of its transformation process. To facilitate the decarbonization goals through digitalization, Eni initiated a large number of digital transformation projects, all of which present cross-cutting challenges for cybersecurity. Consequently, the company developed a global cybersecurity approach to protect industrial control system (ICS) and information and communications technology (ICT) assets and let the IT/OT convergence happen, while protecting ICS from classic ICT threats and thus enabling the business transformation. Eni takes a risked-based approach to cybersecurity that is centred on its strategic vision and aligned with major corporate strategy drivers. It includes protecting key industrial assets, ensuring compliance readiness, employing performance models to ensure continuous improvement, using a resiliency-first approach to monitoring and a rapid services response to guarantee business continuity, and allowing business to leverage emerging technologies.

Reporting and communicating with the Eni risk committee is an important part of the maturity model; providing continuous information and inducting new members are also key success factors. Consequently, a renewed reporting policy has been adapted to the new business needs, with an improved set of risk indicators and the inclusion of risks linked to the human factors of cybersecurity.

Key takeaways: By ensuring continuous alignment with the organization's strategy drivers and establishing clear responsibility, Eni guarantees cybersecurity is an enabler by adapting its cyber organization, culture and practices. Metrics to evaluate key outcomes include: more than 10 cybersecurity reports shared with the risk committee, and more than 10 key risk indicators updated quarterly. So far in 2021, almost 40 cyber projects have been aligned with the company strategy, and cybersecurity competencies have been involved in more the 600 ICT, digital, industrial and business activities.

4.2 Principle OG2 - Resilience by design

The board should promote a *security by design, resilience by design* culture, and should require its management to implement similar standards and values while documenting progress.

Suggested activities for the implementation of resilience by design include to:

- Define cyber-resilience metrics and appropriate incentives for all business units to ensure ownership and commitment to implementing new cyber-resilience requirements in their operations
- Establish a regular cadence of cyber-resilience reporting by the officer accountable for cyber risk and resilience
- Collaborate with business units and risk functions to adapt the cyber-risk posture to business needs
- Establish a cybersecurity awareness programme that is tailored to the needs of each business unit and its unique risks
- Equip personnel with the ability to identify and manage cyber risks
- Ensure cyber resilience, protection, detection and response capabilities are integrated with technical and business activities by design.

Suggested metrics can include the:

- Percentage of business unit processes that adopt and integrate cyber-resilience practices by design
- Percentage of employees following cyber-resilience and awareness training (tailored to different levels)
- Percentage of lighthouse projects that serve as a model covering cyber resilience by design
- Average time to detect, respond to and recover from a critical cyber incident leading to a system failure or disruption.

CASE STUDY

Repsol funds lighthouse projects to build allies

Scenario: Under a company-wide digital transformation initiative at Repsol,[12] the company also shaped a new cybersecurity strategy. Its vision focused on integrating resilience into the business design and improving the recovery time after a cyber incident. Instead of focusing only on technical solutions, the new strategy is based on business resilience and risk appetite, and on the World Economic Forum Cyber Resilience in Oil and Gas community's principles for boards.

To this end, the security and business teams collaborated to define resilience metrics and funded lighthouse projects, ensuring resilience was included from the inception phase. When deemed appropriate, the security team sought support from the board to improve training, awareness and resource allocation to deliver value. This collaborative process allowed Repsol to align the needs of the business and security sections and improve cyber-resilience controls.

Key takeaway: Focusing on the business risks resulted in corporate integration and awareness of cybersecurity, while collecting insights and lessons from the World Economic Forum community to adopt a more holistic approach to cyber resilience.

4.3 Principle OG3 - Corporate responsibility for cyber resilience

The board should encourage management to examine cyber risks to the organization and the broader ecosystem, examine the organization's cyber culture and practices, and explore how to manage these risks.

Suggested activities for the implementation of corporate responsibility for cyber resilience include to:

- Collaborate with other business unit designees and individuals who have the responsibility to integrate cyber resilience in their processes
- Take steps to address internal cyber risk for supply chain partners and the overall ecosystem should the organization experience an attack or breach
- Augment existing business continuity plans with offline recovery measures, out-of-band communication methods and independent recovery sites to cover cybersecurity-related events and increase resilience by design
- Establish ecosystem-wide collaboration and resilience plan activities.

Suggested metrics can include the:

- Number of critical/high cyber risks related to suppliers/business partners by status (accepted, avoided, mitigated, transferred)
- Number of cyber incidents detected/shared within the ecosystem and actions in place to remediate reported vulnerabilities per quarter
- Frequency of budgeting and resource allocation reviews ensuring adequate reflection of the organization's cyber-risk appetite
- Number of cyber-incident scenarios included in the business continuity and disaster recovery plans.

CASE STUDY

Saudi Aramco's integrated approach drives home cyber-risk management

Scenario: Saudi Aramco's board of directors views cyber risks as a business risk of paramount priority. To ensure it is prioritized throughout the organization, cybersecurity must be reported upon and overseen by the board of directors and executive management, to drive cultural resilience and accelerate risk-mitigation efforts.

To enable these changes, the board established a corporate cyber-risk management function to identify, assess, manage and report on cyber risks, and integrated this function in the enterprise risk-management organization. To build a resilient culture, Saudi Aramco then established the Awareness and Behaviour Management function to create a cyber-aware culture, and implemented cyberattack simulation programmes tailored to various stakeholder segments, including executive management, to train them on how to respond and withstand social engineering and attack attempts.

Key takeaway: This approach has resulted in a notable increase in corporate awareness of cybersecurity and resilience against social engineering tactics.

4.4 Principle OG4 - Holistic risk-management approach

The board should ensure that cyber risks are managed and mitigated across the oil and gas ecosystem by providing an adequate mandate, funds, resources and accountability for cyber-resilience programmes and reporting.

Suggested activities for the implementation of holistic risk management include to:

- Identify cyber risks posed within the supply and value chain and work with relevant partners to mitigate their vulnerabilities
- Define and quantify cyber-risk tolerance in collaboration with other business units
- Perform an end-to-end review of the supply- and value-chain dependencies and highlight blind spots and high risks related to cyberthreats
- Ensure risk-management actions and tools follow a consistent holistic approach adopted and accepted across the ecosystem (e.g. security assessments, questionnaires and audits)

- Adopt a common risk framework recognized by the industry, such as the ISO/IEC 27000[13] series, the NIST Cybersecurity Framework[14] or C2M2 maturity models.[15]

Suggested metrics can include the:

- Percentage of strategic or critical suppliers and partners assessed (cyber-resilience due diligence) and with security clauses embedded in their contract
- Number of critical systemic risks (affecting the industry as a whole) covered by the organization's risk analysis
- Frequency of risk assessments conducted for critical business assets, functions and suppliers and business partners, e.g. based on the business impact analysis information
- Number of critical and high cyber risks for critical assets, functions and suppliers
- Number of critical assets covered by the risk-management process.

CASE STUDY

Halliburton's scalable process on cyber-risk acceptance

Scenario: Halliburton documents cyber-risk management and treats cyberthreats as a hazard to business operations. To ensure cybersecurity is a top priority, Halliburton performs security reviews as part of its procurement and building process with four distinct steps: request, assess, approve and track.

When a request is made, Halliburton teams conduct a risk-based assessment grounded in a stable, reliable, repeatable and scalable controls library, taking into account factors like data classification and business process criticality.

The process then requires formal approval from the business, legal and IT departments, with defined levels depending on the degree of risk. Finally, Halliburton uses monthly and quarterly executive reporting to track cyberthreats, including remediation and expiration.

Key takeaways: This repeatable and scalable process ensures the consistent application of risk-based controls with clearly designated responsibilities for risk assessment and cross-functional risk ownership.

4.5 Principle OG5 - Ecosystem-wide collaboration

The board should encourage and empower its management team to create a culture of collaboration for the effective oversight, monitoring and control of ecosystem-wide risks.

Suggested activities for the implementation of the principles of ecosystem-wide collaboration for boards include to:

- Collaborate with ecosystem partners to develop, improve and adopt unified approaches informed by industry frameworks, standards and tools
- Engage in and report on interaction with policy-makers and global standards organizations to make ecosystem-wide collaboration easier
- Engage in or lead cyber-resilience communities and initiatives (under the stewardship of industry, national or international organizations) that encourage information sharing, strengthen collaboration across the ecosystem and drive collective action
- Collaborate with ecosystem stakeholders and actively participate in system-wide cybersecurity information-sharing bodies on cybersecurity topics, e.g. the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC), the Operational Technology Information Sharing and Analysis Center (OT-ISAC), the American Petroleum Institute (API), the European Union Agency for Network and Information Security (ENISA), etc.

Suggested metrics can include the:

- Frequency of events and engagements with ecosystem and industry peers
- Frequency of meetings with security officials and cyber-response experts, including policy-makers, national security and intelligence officials, private-sector cyber-response and legal experts
- Number of threat intelligence reports and briefings exchanged with peers across the ecosystem.

CASE STUDY **Saudi Aramco promotes cybersecurity information sharing**

Scenario: Saudi Aramco encourages a culture of collaboration and information sharing at the highest levels of its leadership. Both within Saudi Aramco and with external partners, the company promotes the exchange of lessons learned from challenging cyber-resilience situations and success stories, to better foster collaboration, improvement and knowledge sharing. For example, Saudi Aramco formed a consortium for information sharing with some of its regional partners to accelerate readiness against cyberattacks, and founded benchmarking groups in the industry to periodically exchange knowledge and best practices.

Externally, Saudi Aramco has established or participated in multiple cybersecurity-focused partnerships to unlock new opportunities that will elevate the cyber maturity and posture of its organization. Saudi Aramco believes that these exchanges are necessary to accelerate solutions to the industry's pressing challenges and risks.

In addition, Saudi Aramco launched an annual seminar for its third parties to share cybersecurity best practices as part of its ecosystem collaboration to strengthen its supply chain's cybersecurity posture.

Key takeaway: By founding regional cybersecurity information-sharing consortiums and collaborating with various groups in the industry and the World Economic Forum, Saudi Aramco is able to continuously improve its cybersecurity programme, increase cyber hygiene across its supply chain and shape the future of cybersecurity in the industry.

4.6 Principle OG6 - Ecosystem-wide cyber-resilience plans

The board should encourage management to create, implement, test and improve collective cyber-resilience plans and controls with other members of the ecosystem. These plans should consider preparedness and protection (e.g. defence in depth strategies) in conjunction with response and recovery capabilities.

Suggested activities for the implementation of the principles of ecosystem-wide cyber-resilience plans include to:

- Develop a cyber-resilience plan as one of the organization's strategic priorities, in close collaboration with all business function and unit leaders, and explicitly incorporate the board's role
- Set a regular cadence of reporting on cyber-resilience plans, to include vital updates, testing frequency and results
- Conduct regular cybersecurity exercises and tests on cyber resilience that include systemic failure and subsequent recovery as a component or focus of the exercise
- Ensure that the cybersecurity strategy and programme is linked with internal and external sources, the management of incidents, and response and recovery capabilities (from a people, process and technology perspective).

Suggested metrics can include the:

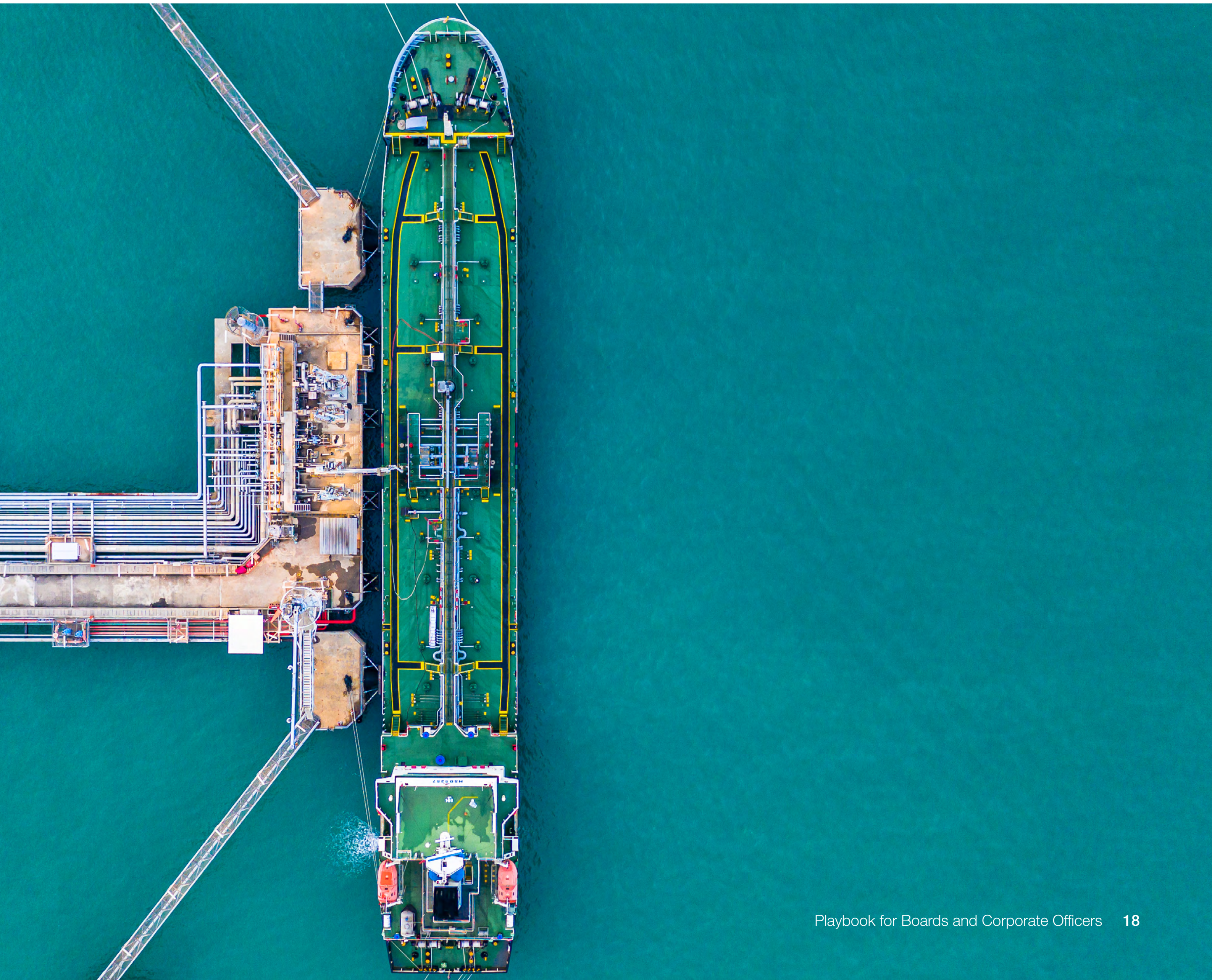
- Number of tests conducted and adopted corrective measures
- Number of hours of interruption or disruption of essential business services, including the financial impacts of disruptions
- Percentage of critical open actions and closed actions resulting from cybersecurity preparedness exercises, including systemic failure testing as a component or focus of the exercises
- Percentage of critical systems that implemented and successfully tested contingency and disaster recovery plans this quarter.

5 Conclusion

Cyber resilience is an essential part of appropriate diligence when conducting business in the oil and gas sector. Digitization has improved almost all parts of the value chain, creating unprecedented efficiencies and new operating models. Yet unless the oil and gas value chain can withstand or recover from cyber risk, the risk may have disastrous physical, environmental and safety consequences. Both within enterprises and as a sector overall, businesses in the oil and gas industry need to develop their cyber resilience further to protect the bottom line. The six cyber-resilience principles for oil and gas boards will help organizations systematically and comprehensively adopt resilient practices and corporate cultures, while preparing them to meet the increasing environmental protection, social and governance expectations of shareholders and society.

Boards can manage and mitigate cyber risks by ensuring certain steps are taken within their organizations and by working with partners across industry. Each organization will need to consider its own maturity as it works towards improving cyber resilience. Organizations that implement strong governance, ensure resilience by design, build a resilient culture and consider cyber risk holistically when allocating resources will be better able to weather attacks, accidents and disruptions. Organizations that further consider how to gain and share insights with other actors in the oil and gas sector and how to support other links in the value chain will help mitigate shared risks and prevent incidents from becoming industry-wide disruptions.

Fostering strong cyber resilience will reduce risk across the oil and gas industry and enable automation and digitization to continue improving efficiencies and enhance reliability in competitive supply chains. It is up to industry leaders to chart the course to that stable future.



Appendix A: General cyber-resilience principles for boards[16]

Description of general principles for boards

PRINCIPLE 1

Responsibility for cyber resilience

The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber-resilience committee).

PRINCIPLE 2

Command of the subject

Board members receive cyber-resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts upon request.

PRINCIPLE 3

Accountable officer

The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and on progress in implementing cyber-resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

PRINCIPLE 4

Integration of cyber resilience

The board ensures that management integrates cyber-resilience and cyber-risk assessments into the overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

PRINCIPLE 5

Risk appetite

The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with the corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

PRINCIPLE 6

Risk assessment and reporting

The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the board's cyber-risk framework.

PRINCIPLE 7

Resilience plans

The board ensures that management supports the officer accountable for cyber resilience through the creation, implementation, testing and ongoing improvement of cyber-resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

PRINCIPLE 8

Community

The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

PRINCIPLE 9

Review

The board ensures that a formal, independent cyber-resilience review of the organization is carried out annually.

PRINCIPLE 10

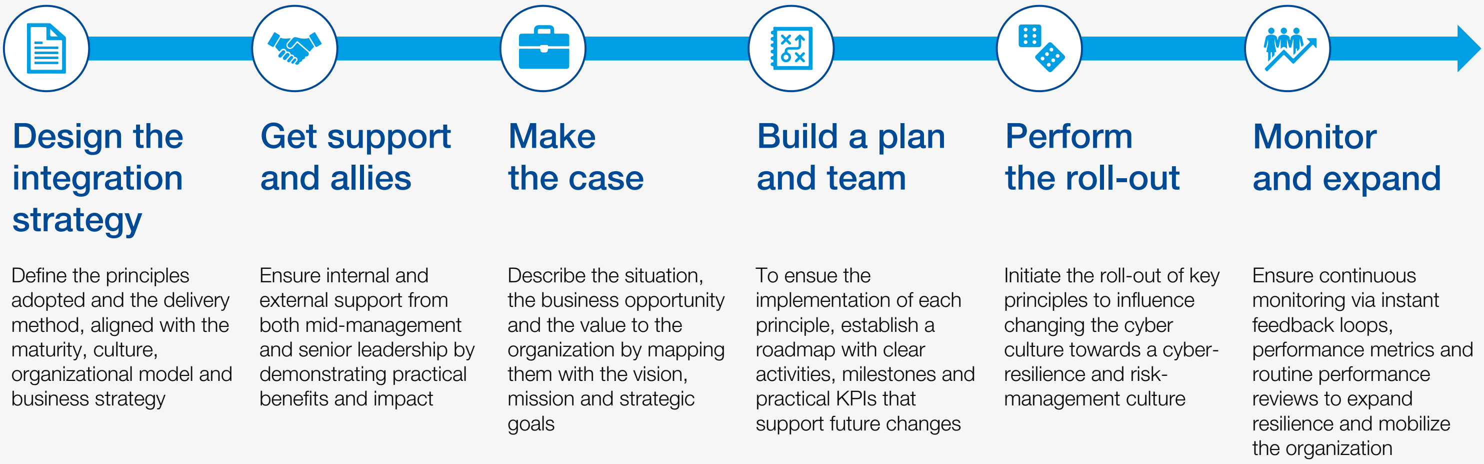
Effectiveness

The board periodically reviews its own performance on the implementation of these principles or seeks independent advice for continuous improvement.

Appendix B: How to operationalize the principles

To implement these principles and fully realize their intended benefits, cyber resilience must not be an after-thought but must be embedded into an organization's culture and incorporated into all aspects of a business's norms. Because corporate officers and managers responsible for cyber resilience frequently face resistance to changing corporate policies and attitudes, they will often need a board mandate operationalizing cyber-resilience principles. To shift deeply embedded corporate mindsets, managers can take a gradual approach (Figure 2) to introduce cyber-resilience best practices within oil and gas organizations.

FIGURE 2 **Approach for adopting and implementing the cyber-resilience principles across the oil and gas industry**



Design the integration strategy

Define the principles adopted and the delivery method, aligned with the maturity, culture, organizational model and business strategy

Get support and allies

Ensure internal and external support from both mid-management and senior leadership by demonstrating practical benefits and impact

Make the case

Describe the situation, the business opportunity and the value to the organization by mapping them with the vision, mission and strategic goals

Build a plan and team

To ensue the implementation of each principle, establish a roadmap with clear activities, milestones and practical KPIs that support future changes

Perform the roll-out

Initiate the roll-out of key principles to influence changing the cyber culture towards a cyber-resilience and risk-management culture

Monitor and expand

Ensure continuous monitoring via instant feedback loops, performance metrics and routine performance reviews to expand resilience and mobilize the organization

Source: World Economic Forum

1. Design the integration strategy

Define a strategy that will effectively integrate and ensure the adoption of new cyber policies and principles.

How to implement this phase towards cyber resilience:

- Define a delivery methodology around four key pillars within the organization: risk posture, internal culture, organizational model and business strategy

- Before introducing actions to a wider community, assess the internal maturity and risk posture of the organization to accurately prioritize the efficacy of principle implementation actions

- Ensure the cyber-resilience principles are aligned and integrated with the business's strategy, vision and mission by understanding how cybersecurity can support and enable each business unit's core competency

- Understand the organizational operating model and structure to verify which key stakeholders are required for rapid and successful adoption

- Select a delivery-model strategy that integrates well into the organization’s internal culture to ensure the efficient adoption and implementation of cyber-resilience principles (e.g. a tailored and phased model vs all-in-one implementation).

2. Get support and allies

Ensure internal support from both mid-management and senior leadership by demonstrating the cyber risks of their business unit while leveraging the board mandate, and clarifying the specific expectations and requirements needed to support the board mandate; this important phase helps to secure buy-in from key stakeholders by illustrating the value of the principles in unique situations.

How to implement this phase towards cyber resilience:

- Secure support from senior leadership by making the case for and demonstrating the importance of cyber resilience to the responsible board member

- Identify key supporters from multiple stakeholders across the organization that are crucial for the implementation of the principles (e.g. risk officer and audit team responsible person)

- Get internal buy-in from key business heads when building a strategic plan by illustrating the relevance and benefits to their businesses

- Provide resources and funding support for pilot or lighthouse projects with dedicated cybersecurity funds to help ensure operational budgets are allocated when adopting cyber-resilience measures

- Integrate cyber-resilience principles into existing governance processes for seamless and more rapid adoption (e.g. leveraging the safety culture and other mature disciplines).

3. Make the case

To maintain senior leadership support and engagement, describe cyber resilience as a business opportunity of value to the organization by mapping a new cyber policy with the company’s vision, mission and strategic goals.

How to implement this phase towards cyber resilience:

- Communicate the complexity and urgency of implementation, e.g. illustrating the risks for the organization and business unit, and citing competitor actions against the industry benchmarks

- Coordinate with identified internal allies to ensure a collaborative and holistic proposal when communicating and reporting to the board

- Reiterate the benefits of cyber resilience to the board by demonstrating business value through quantifying and qualifying the risks and rewards for the organization through practical examples

- Set clear goals by clarifying performance measurement points and timely key performance indicators, and defining regular reporting (from monthly to biannually)

- Highlight the value and benefits of long-term cyber resilience by reiterating the relevance of the principles for boards.

4. Build a plan and team

To ensure the efficient adoption and implementation of the principles for boards, establish a roadmap with clear activities, milestones and practical key performance indicators with mechanisms that support future changes.

How to implement this phase towards cyber resilience:

- Select a cross-functional team to manage an implementation roadmap based on the organization’s complexity and culture, and each of the principle’s goals
- Adapt and validate the plan (if needed) by setting key deliverables and measurement points and a well-defined reporting and metric communication plan
- Define the delivery model by considering internal change management, business process engineering and the delivery method (e.g. using agile methodology and annual business planning)
- Ensure the team understands the value of the principles and champions the roadmap by applying individual goals and embedding cybersecurity responsibility within each role.

5. Perform the roll-out

Initiate the roll-out of the key cyber-resilience and risk-management principles to influence changing the cybersecurity culture by following a defined integration strategy.

How to implement this phase towards cyber resilience:

- Introduce, implement and embed cyber-resilience principles into a target operating model
- Leverage pilot, lighthouse and existing projects to integrate cyber-resilience programmes into new developments
- Tailor training to a wide range of staff members, including board members, to set comprehensive expectations and awareness of inherent cyber risks.

6. Monitor and expand

Ensure continuous monitoring through instant feedback loops, while providing key performance metrics and carrying out routine performance reviews needed to expand cyber resilience throughout the organization.

How to implement this phase towards cyber resilience:

- Ensure continuous communication to key stakeholders on the value of ongoing and future cyber-resilience projects and the achievement of the organization’s cybersecurity goals
- Ensure continuous reporting and feedback to the board, recalling initial goals, providing simple measurements and communicating progress and the overall value
- Monitor leading indicators (e.g. project budget, capacity availability) and remove identified obstacles before they can negatively impact implementation
- Monitor and review defined performance indicators and when needed adapt them to support cybersecurity expansion.

Appendix C: Taxonomy

Term	Definition
Board and board of directors	Corporate fiduciaries responsible for supervising management strategy as well as identifying and planning responses to enterprise-wide risks affecting a company and its value to stakeholders and shareholders[17]
Corporate officer/manager responsible for cyber resilience	Represents the accountable officer as the corporate officer accountable for reporting on the organization's capability to manage cyber resilience and on progress in implementing cyber-resilience goals.[18] The chief information security officer (CISO) is often the individual within the organization who is responsible for overseeing the organization's cyber-resilience programme aimed at protecting digital infrastructure and assets against cyberthreats and ensuring the continuity of business operations. This officer is usually a senior executive essential in leading and overseeing the company's overall cyber-resilience strategy and reporting to and advising the board of directors regarding cyber risks[19]
Cyber resilience	A dimension of cyber-risk management, representing "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources"[20]
Cyber risk	Probable loss event that materializes when a cyberthreat affects an asset of value and results in a material impact on an organization; cyber risk can be measured as the probable frequency and the probable impact of a loss event[21]
Information technology (IT)	Covers any form of technology – that is, any equipment or technique used by a company, institution or any other organization that handles information[22]
Operational technology (OT)	Monitors and manages industrial process assets and manufacturing/industrial equipment; OT has existed for much longer than IT – ever since people started to use machinery and equipment powered by electricity in factories, buildings, transportation systems, the utility industry, etc.[23]
Risk appetite	The organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives; risk tolerance can be influenced by legal or regulatory requirements
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk management	Coordinated activities to direct and control an organization with regard to risk

Appendix D: Cyber Resilience in Oil and Gas Strategy and Culture Working Group

The working group consists of senior executives from the oil and gas industry tasked with establishing a blueprint for evaluating cyber risk and enhancing cyber resilience across the industry. The following individuals led invaluable in-depth discussions to illuminate the industry's best practices and create new solutions that help corporate leaders address cyber risk.

Working group chair

Leo Simonovich
Vice-President and Global Head, Industrial Cyber and Digital Security, Siemens Corporation, USA

Working group members

Aker BP, Norway: Sigmund Kristiansen
American Petroleum Institute, USA: Suzanne Lemieux
Baker Hughes, Italy: Angela Grisafi
Boston Consulting Group, USA: Stefan Deutscher, Walter Bohmayr
BP, UK: Yolande Young
Cognite, Norway: Jakob Eide
Cyber Security Agency of Singapore, Singapore: Thian Chin Lim
Cybersecurity and Infrastructure Security Agency, USA: Robert Watson, Gabriel Hengel
Ecopetrol, Colombia: Alberto Leon Lozano, Edgardo Arrieta Arteta
Eni, Italy: Giorgio Medina, Dario Pagani
EnQuest, UK: Ali Talpur, Michael Thomson
Galp Energia, Portugal: Luis Filipe Morais
Global Resilience Federation, Singapore: AJ Eserjose, John Lee
Halliburton Company, USA: Mary Rose Martinez
HCL Technologies, India: Neelakarun Asari
Institute for Security and Safety, Germany: Guido Gluschke, Swantje Westpfahl
Kuwait Oil Company, Kuwait: Reem Faraj Al-Shammari
Maire Tecnimont, Italy: Max Panaro
Occidental Petroleum Corporation, USA: Fakhry Nusiebeh, Yanni Charalambous
Office of Gas and Electricity Markets (Ofgem), UK: Mohammed Zumla
Palo Alto Networks, USA: Haider Pasha
Pan American Energy, Argentina: Maria del Rosario Romero
Petronas, Malaysia: Muhittin Hasancioglu
PwC, USA: Harshul Joshi
Repsol, Spain: Javier Garcia Quintela
Royal Dutch Shell, Netherlands: Vincent van Schaik
Royal Vopak, Netherlands: Arno Sevinga
Saudi Aramco, Saudi Arabia: Basim Al-Ruwaii, Noura Alajmi
Schneider Electric, France: Mansur Abilkasimov
SecurityScorecard, USA: Alex Rich, Mike Wilkes
Siemens Energy, USA: John Ellis, John LaRue
Suncor Energy, Canada: John Hill, David Craig
Trafigura Group, Switzerland: Mark Swift

Contributors

The World Economic Forum Cyber Resilience in Oil and Gas community is a global, multistakeholder endeavour comprising oil and gas organizations, businesses, providers and governments.

Lead authors

Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum

Andrew Gumbiner
Adviser, Policy Strategy, Siemens Energy, Germany

Leo Simonovich
Vice-President and Global Head, Industrial Cyber and Digital Security, Siemens Corporation, USA

Wesam Al-Zamil
Lead, Cybersecurity, Saudi Aramco, Saudi Arabia

Advisory team

Christophe Blassiau
Senior Vice-President, Cybersecurity; Global Chief Information Security Officer, Schneider Electric, France

Georges De Moura
Head, Industry Solutions, Centre for Cybersecurity, World Economic Forum

Pedro Gomez
Head, Oil and Gas Industry, World Economic Forum

Khalid Al-Harbi
Chief Information Security Officer (2018-2021), Saudi Aramco, Saudi Arabia

Maciej Kolaczkowski
Community Lead, Oil and Gas Industry, World Economic Forum

Robert Lee
Chief Executive Officer, Dragos, USA

Hisham Al-Muhareb
Head, Cybersecurity Governance, Saudi Aramco, Saudi Arabia

Anders Rimstad
Chief Security Officer, Aker, Norway

Endnotes

1. World Economic Forum, *The Global Risks Report 2021*, 16th Edition, 2021, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (accessed 20 April 2021).
2. Kaspersky Industrial Control Systems Cyber Emergency Response Team (ICS CERT), *Threat landscape for industrial automation systems*, H1 2020, https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf (accessed 20 April 2021).
3. Juniper Research, "Industrial IOT Connections to Reach 37 Billion Globally by 2025, as 'Smart Factory' Concept Realised", Press release, 2 November 2020, https://www.juniperresearch.com/press/industrial-iot-iiot-connections-smart-factories (accessed 26 April 2021).
4. IBM, "IBM X-Force Threat Intelligence Index", 2020, https://www.ibm.com/security/data-breach/threat-intelligence (accessed 20 April 2021).
5. IBM Security and Ponemon Institute, *Cost of a Data Breach Report 2020*, 2020, p. 12, https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf (accessed 20 April 2021).
6. Ponemon Institute, "The State of Cybersecurity in the Oil & Gas Industry: United States", Executive Summary", 2017, https://assets.new.siemens.com/siemens/assets/api/uuid:4ec3d46c-234e-4f48-9bc7-aef5889dcaba/version:1599660343/ponemoncyberreadinessinoilgasfinal.pdf (accessed 20 April 2021).
7. World Economic Forum, *Advancing Cyber Resilience: Principles and Tools for Boards*, Future of Digital Economy and Society System Initiative, In collaboration with the Boston Consulting Group and Hewlett Packard Enterprise, 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (accessed 20 April 2021).
8. World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, Centre for Cybersecurity and Electricity Industry Community, In collaboration with Boston Consulting Group, 2019, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf (accessed 20 April 2021).
9. World Economic Forum, National Association of Corporate Directors (NACD) and Internet Security Alliance, *Principles for Board Governance of Cyber Risk*, Insight Report, In collaboration with PwC, 2021, http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf (accessed 20 April 2021).
10. Defence in depth is a type of cybersecurity in which several independent layers of security controls are used so that if one fails, another will take effect.
11. Ponemon Institute, "The State of Cybersecurity in the Oil & Gas Industry: United States", Executive Summary, 2017, https://assets.new.siemens.com/siemens/assets/api/uuid:4ec3d46c-234e-4f48-9bc7-aef5889dcaba/version:1599660343/ponemoncyberreadinessinoilgasfinal.pdf (accessed 21 April 2021).
12. Repsol, "The digital transformation of Repsol", https://www.repsol.com/imagenes/global/en/digital_transformation_dossier_tcm14-144286.pdf (accessed 21 April 2021).
13. International Organization for Standardization, "ISO/IEC 27001 Information Security Management", https://www.iso.org/isoiec-27001-information-security.html (accessed 22 April 2021).
14. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, "Cybersecurity Framework", https://www.nist.gov/cyberframework (accessed 22 April 2021).
15. U.S. Department of Energy (DOE), *Cybersecurity Capability Maturity Model (C2M2) Version 1.1*, 2014, https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf (accessed 22 April 2021).
16. See also World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, op. cit.
17. National Association of Corporate Directors and Internet Security Alliance, *Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards*, 2020, p. 6, http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf (accessed 16 April 2021).
18. World Economic Forum, *Advancing Cyber Resilience: Principles and Tools for Boards*, op. cit., Principle 3, p. 8.
19. World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Playbook for Boards and Cybersecurity Officers*, Shaping the Future of Cybersecurity and Digital Trust, In collaboration with Accenture and the Electricity Industry Community, 2020, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Playbook_for_Boards_and_Cybersecurity_Officers_2020.pdf (accessed 16 April 2021).
20. National Institute of Standards and Technology (NIST), *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, Volume 2, 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf (accessed 16 April 2021).
21. Freund, Jack, and Jack Jones, *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, 2014.
22. See World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Playbook for Boards and Cybersecurity Officers*, op. cit.
23. Ibid.

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org