KPMG

DRILLING DOWN

Oil and Gas Magazine

First edition

Articles include:

Top risks facing the oil and gas industry in 2022 — and what you can do about it

Accelerating OT security for rapid risk reduction

Bringing cyber process hazard analysis to the digital era

Safeguard your digital environments from all angles

KPMG International

home.kpmg/drillingdown

Foreword

Welcome to the first edition of KPMG's new oil and gas magazine, *Drilling Down* — designed to be of interest to anyone with a connection to the industry. We hope it will bring you valuable topical insights and promote discussion and debate around the key issues facing our sector.

The current global geopolitical tensions combined with intense uncertainty in supply chains have resulted in a rise in hydrocarbon prices, giving the industry a temporary financial break. This price environment is not all positive as it creates significant challenges as external scrutiny increases. Given this fraught environment, our view is that the industry should continue to strengthen its defenses and controls around an array of risks ranging from geopolitics to cyber and talent.

In this issue, we hone in on some of these specific risks, particularly cyber. At KPMG we believe the oil and gas industry is a principal target for cyber threats and the industry must plan for future threats. Our authors put forward detailed views on the nature of the risks confronting oil and gas and related industrial businesses and set out best practice approaches to mitigate them.

"Given this fraught environment, our view is that the industry should continue to strengthen its defenses and controls around an array of risks ranging from geopolitics to cyber and talent."

Regina Mayor
Global Head of Energy
KPMG International

More broadly, there is an existential risk facing oil and gas companies. Negative public sentiment — from investors and the public at large — continues to grow. Demands to boycott the industry are increasing — encompassing everything from museums to sporting competitions. These views are more prevalent in well developed economies but do not really represent those less developed economies where 759 million people[2] still do not have access to reliable energy supply, or other economies where revenues from hydrocarbons fill state reserves and contribute to a redistribution of wealth by lifting millions of people out of poverty.

In my view, the global oil and gas industry has a unique opportunity to shift the narrative — becoming more proactive around all the things the industry can do to drive the planet toward a net zero reality. The industry as a whole could do more to promote what it is doing for the common good — to be more proactive in its communications and not as reactive.

The Statement on the Purpose of a Corporation (published by the American Business roundtable, August 2019) acknowledges the need to go beyond the creation of shareholder value to focus also on investing in employees, supporting communities, delivering value to customers and dealing fairly and ethically with suppliers. In my view the industry could benefit from a similar oil and gas specific statement, working with public companies, state regulators and industry organizations to promote a new industry paradigm around the following themes:

— The world needs energy to power economic growth well into the future. The industry has enabled substantial improvement of everyday lives.

— The lives of 40 percent of the global population can be significantly improved by having reliable access to affordable energy.

— Gas is a significantly cleaner fuel than coal, less from the point of view of carbon emissions and more from the perspective of air quality — a highly topical issue in India and China but also in Western economies.

— The oil and gas industry is focused on developing carbon capture processes and technologies to mitigate negative climate effects.

— The industry is actively rebalancing its portfolio of assets towards cleaner fuels by increasing the role of gas and alternative energy assets such as wind, solar, etc.

— The industry plays a meaningful role in sustaining millions of people by funding government budgets in many oil and gas dependent nations and contributes to sustaining these economies.

The promotion of these themes to the public at large through a concerted industry effort would help mitigate negative perception risks by showcasing all that the industry does to make a meaningful contribution to all its stakeholders. We plan to explore these issues in more detail in a later edition.

I hope *Drilling Down* becomes a useful source of ideas for oil and gas professionals around the world. Do please get in touch if it stimulates any thoughts or questions that you would like to discuss.

The Statement on the Purpose of a Corporation (published by the American Business roundtable, August 2019) acknowledges the need to go beyond the creation of shareholder value to focus also on investing in employees, supporting communities, delivering value to customers and dealing fairly and ethically with suppliers."

[2] World Bank

Contents

05

Top risks facing the oil and gas industry in 2022 — and what you can do about it

06 Seven keys to get your company ready for the unexpected

07 The uncertain state of the world's oil supply

08 Impact of rising tensions with Russia on Europe's gas supply and prices

09 Potential impact of global decarbonization efforts on the oil and gas industry

10 "Activist" impact on the oil and gas industry

11 Hope for the best, prepare for the worst

12 Final thoughts: Navigating through the uncertainty

12 Risks on the horizon: The search for talent

14 Tips for improving employee recruiting and retention

14 About the authors

15

Accelerating OT security for rapid risk reduction

15 The convergence of OT and IT

17 Top-down and bottom-up approaches

19 Eight key questions

20 Leveraging emerging technologies

21 Getting the people and teams approach right

22 Four takeaways

23 How KPMG firms can help

23 About the authors

24

Bringing cyber process hazard analysis to the digital era

26 A rising threat landscape

27 Strengthening defenses through cyber PHA

29 The benefits of cyber PHA

29 Cyber PHA on the regulatory radar

31 How KPMG firms can help

31 About the authors

32

Safeguard your digital environments from all angles

34 Cybercrime is big and growing

35 Zero trust basics: The perimeter-less border/ Trust no one

36 Key potential benefits of zero trust

37 Getting started on your zero trust journey

39 Continue on your zero trust journey — or start today

40 How KPMG firms can help

41 About the authors

Top risks facing the oil and gas industry in 2022

and what you can do about it

By: Raad Alkadiri, Regina Mayor and Stefano Moritsch

Seven keys to get your company ready for the unexpected

In my nearly 30 years of looking at oil markets, I can't think of a time when geopolitically there was as much uncertainty over potential high and low points in terms of prices, supply and demand."

Raad Alkadiri
Managing Director, Energy,
Climate & Resources, Eurasia Group

The oil and gas industry perpetually seems rife with uncertainty and potential volatility. Between rising and diminishing consumer demand, price fluctuations, and of course, geopolitical issues where one global supplier or another threatens to cut off supplies, every day holds surprises and risks. But 2022 seems to be upping the stakes in terms of risk and uncertainty. The Russian invasion of Ukraine is a reminder of how quickly changes in the geopolitical landscape can impact energy prices. Negotiations over a new nuclear deal with Iran add another complication to the energy outlook.

At the same time, the lingering impact of COVID-19 is still being felt. While cases seem to be moderating in many parts of the world, the supply chain and vaccine mandate issues are ongoing, and China's "zero-COVID" health policies pose a major risk for energy demand growth. Add to this mix the increasing measures across the globe promoting decarbonization efforts and growing activist pressure over climate change.

What you are left with is a lot of uncertainty and unanswerable questions. This article drills down into the top risks looming over the oil and gas industry for the remainder of 2022 and attempts to provide answers and some steps companies can take to prepare for them.

The uncertain state of the world's oil supply

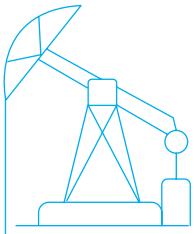
In 2022, we are seeing the results of a supply shock with a tight oil supply and supply disruptions driving prices well north of $100/barrel to near record highs. But believe it or not, there is a scenario where we can see a situation with excess supply later this year or early next. Volatility will likely be with us for some time.

The potential oversupply scenario happens if OPEC makes good on its commitment to continue unwinding the supply cuts it made in 2020, and U.S. unconventional production grows as much as some analysts are forecasting. If these events occur, organizations may end up with an oversupply of oil, with as much as an extra 6.4 million barrels per day late this year. Add to that a potential new nuclear agreement with Iran and the volume of new oil coming onto the market this year will be even higher; some estimates have Iranian exports growing by up to a million barrels a day within a few months if a new pact is struck. (Of course, if a U.S.-Iran deal occurs, it might factor into OPEC's decision to continue unwinding its cuts.)

On the flipside, of course, is Russia's invasion of Ukraine, and the risks that it will lead to a further curtailment of Russian oil exports — including more drastic measures from Europe. Outrage over the invasion has led to some self-sanctioning by western buyers; the U.S. has already initiated a ban on Russian oil, and the European Union (EU) is actively contemplating one. The IEA currently predicts as much as 3MM BPD of Russian exports could be taken off the market. On to the demand side, higher energy prices from the Ukraine crisis could have a knock-on effect on international economic growth.

Meanwhile, China appears to be sticking with its "zero COVID" policy, which includes severe lockdowns and other business-limiting measures. What's more, President Xi's economic and environmental policies may slow down China's economic expansion, and therefore decrease its demand for oil. This could have a ripple effect on the global economy, making forecasts of increased global oil demand of 3.3 million barrels per day illusory.

For the time being, we're still experiencing a tight oil market although many are forecasting a growing oil surplus beginning in the second half of the year.[1]



On the demand side, **higher energy prices from the Ukraine crisis** could have a knock-on effect on international economic growth.

[1] Reuters, OPEC+ trims forecast for 2022 oil market surplus in latest data, 27 February 2022

Impact of rising tensions with Russia on Europe's gas supply and prices

Russia's invasion of Ukraine has prompted the U.S. and EU to impose severe economic sanctions on Russia.

This tense geopolitical issue is casting a long shadow over gas supplies and prices, especially in Europe.

Reductions in Russian spot sales of gas to Europe in late 2021 contributed to an energy crunch and record natural gas prices in the EU. The fear now is that fighting in Ukraine and the impact of sanctions will disrupt much larger volumes of gas, keeping prices high and undermining EU economic growth this year. If Moscow were to retaliate to U.S. and EU sanctions by cutting off all gas exports to Europe, the results would be even more onerous for European economies.

How this crisis plays out in the longer-term will have significant implications for the energy mix in Europe over the next 5–10 years. There is one school of thought that Europe will delay implementation of some of its key "green transition" energy policies to avoid short-term pain. On the other hand, many believe that this vulnerability will motivate EU countries to double down and accelerate the pace of their transition to renewables and clean energy in order to decouple from reliance on Russian gas. This will likely have a big geopolitical impact in terms of Russia's leverage over Europe, and also in terms of where Russia would sell its oil and gas supplies.

Is it politically feasible for EU governments to do this? Can the EU accept the potential short-term pain in terms of increased prices and limited gas supplies in order to gain a long-term advantage? And what steps will it take to ease the burden on its citizens?

For example, Germany has said that, in light of the Ukraine invasion, it will not certify the Nord Stream 2 gas pipeline, which was designed to deliver more Russian gas to the EU.[2] The bloc is also taking steps to displace some Russian gas with supply from the U.S. and Qatar until its transition efforts are further along and bear more fruit. These are all questions that many hope will be answered as the year moves forward.

"In some parts of the world, energy transformation and energy security are seen as being synonymous rather than disruptive."

Regina Mayor
Global Head of Energy
KPMG International

[2] Reuters, Germany freezes Nord Stream 2 gas project as Ukraine crisis deepens, 22 February 2022

Potential impact of global decarbonization efforts on the oil and gas industry

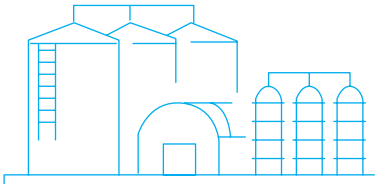
Beyond environmental and economic considerations, geopolitical volatility is, more than ever, triggering a fundamental re-think of energy strategy around the globe. National security interests will likely determine the speed and direction of the decarbonization journey"

Stefano Moritsch
Global Geopolitics Lead
KPMG International

When it comes to global energy transformation efforts, it seems like it is one step forward and two steps back. While global energy transformation efforts to reduce emissions are being baked into policies around the world, it's not a one-size-fits-all approach and it's happening at different speeds in different countries. And as events in Europe illustrate, politics have a major impact.

Fallout from the Ukraine crisis may accelerate the EU's "Fit for 55" proposals, which aim to reduce greenhouse gas emissions by at least 55 percent by 2030. Meanwhile, China also appears to be willing to put up with higher cost and burdens as it forges ahead with its emission reductions. It turns out that in some parts of the world, energy transformation and energy security are seen as being synonymous rather than disruptive.

Ultimately, the tension between governments' balancing of long-term energy goals and the short-term needs of their citizens will make the road to energy transformation extremely bumpy. Governments will have their work cut out for them in trying to minimize the pain that will likely be caused by the transformation efforts while still making progress on its energy policies.



Fallout from the Ukraine crisis may accelerate the EU's **"Fit for 55"** proposals, which aim to reduce greenhouse gas emissions by at least 55 percent by 2030.

"Activist" impact on the oil and gas industry

It is not just governments that oil and gas companies need to pay close attention to. Environmental and social activists are putting increasing pressure on the industry, questioning its "social license" to operate. This is largely based on the pollution and climate change damage they believe the industry is responsible for.

The industry has dealt with this issue for decades but the increasing attention on the threat of global warming has really increased.

Activist investors are speaking with their pocketbooks and shifting more of their investment dollars toward green energy. Another game changer has been the expansion of social media platforms and new technology that provides activists with the ability to get their message out more widely to the general public and also more directly to corporate executives and board members. In addition, climate activists are also taking to the courts; although the results have been mixed, the potential liability and bad publicity it generates creates great uncertainty and risk for the industry.

As a result, oil and gas companies are feeling intense pressure to respond in terms of capital allocation decisions and strategy out of fear of damage to both their corporate reputation and bottom lines.

A somewhat surprising development that may come out of the private sector continuing to shift its investment focus toward green energy and away from oil and gas is that national oil companies (NOCs) may end up with even more power — at least in the short term. Regardless of what happens in the long term, worldwide energy needs are not decreasing. So while some oil and gas firms may gradually get squeezed out of the market, it may lead to even greater reliance on the NOCs for their production. And this may give them greater political leverage. But NOCs should act judiciously; if they push their advantage too hard, it may backfire and end up with a faster shift away from consumption of oil and gas in the longer term.

Hope for the best, prepare for the worst

It's impossible to predict the future. Who could have imagined the COVID 19 pandemic that's upended the world and the global economy for two years? Or the military invasion of Ukraine by the Russian government that will likely be a profound political and economic global fallout.

Much of what may happen is out of the control of the oil and gas industry. However, the following are some steps you may want to consider taking so that your organization will be as well positioned and prepared as possible regardless of what occurs in 2022.

1. Have an ESG (environmental, social and governance) plan in place to proactively address activist investor and stakeholder concerns. Tackle the issues head-on rather than waiting to respond under pressure.

2. Review your organizations' crisis playbook. Does it include all potential scenarios, and is it updated regularly?

3. Review your organization's commodity risk management philosophy. Prepare for how short and long-term changes in the pricing environment could impact customer and shareholder sentiment, and also government involvement.

4. Understand how proposed legislation and government actions could impact your company: Determine if your organization has the flexibility to shift gears quickly to take advantage of opportunities as political agendas change.

5. Focus on relationship building: Continue or increase efforts to build relationships with all relevant stakeholders, including consumer groups, governments, regulators, and society at large. In the same way, consider industry and cross-industry cooperation efforts to proactively shape reasonable regulation with governments.

6. Get your supply chains in order: Review your current setup and determine how you can reduce disruption and improve resilience.

    - For example, are your operations flexible and resilient enough to adapt and adjust in real-time to changes in trade flows, new regulations, continued COVID-19 disruption, climate change, trade tensions and other geopolitical movements?

    - Is your technology current so you can reduce operating costs, provide visibility, and seamlessly diversify the way customer needs are met?

7. Review your organization's cyber defense protection: The risk of a cyber breach is perhaps the most underestimated above-ground risk in the oil and gas sector. It cuts across political and geographical boundaries and any company, regardless of size, is a potential target. No matter your location or where you operate, you are equally vulnerable to a cyber security breach.

Final thoughts: Navigating through the uncertainty

As this article has highlighted, there hasn't been a time where there's been more uncertainty for oil and gas companies. What is certain, however, is that the world is not going to go back to where it was, and the oil and gas industry will need to change.

There will likely be a continuing push for decarbonization and other climate control efforts, whether by governments or activist and consumer groups, and incremental tweaks to technology may not do the trick.

The speed and intensity of the transformation may be impacted by short-term supply and price issues and geopolitical events, but the future direction is clear. The oil and gas industry will need to change, and you should be taking steps now to prepare for the inevitable.

Risks on the horizon: The search for talent

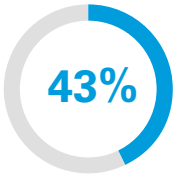
The oil and gas industry has faced a talent shortage for years due to an aging workforce, limited new/young talent entering the industry, and growing competition for talent with the technology industry. This difficulty in getting and retaining talent, which may pose significant issues for the future of the industry, can be attributable to several factors:

The negative perception of the industry: The industry is often cast in a negative light by the media. As a result, many talented individuals tend to shun the industry — although this is by no means universal.

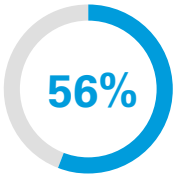
That's why oil and gas companies continue to rely on the experienced crews who often come back after retirement as contractors.

What's more, there may be a need to "import" foreign employees from India, China and Russia, for example, to help fill the breach. But that also may entail a host of political, immigration and security issues.

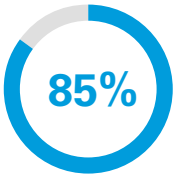
The oil and gas workforce of the future[4]



of current energy workers want to leave the industry altogether within the next five years



of those currently working in oil and gas said they'd consider jobs with renewables organizations



of university students considering a career in the oil and gas industry said it is important that their future employer has policies aimed at addressing climate change and environmental factors[5]

[4] Brunel International/Oil and Gas Job Search, Energy outlook Report 2021–2022

[5] University of Houston, Insights into the Oil and Gas Workforce of the Future

Lack of employees with the "right" skills: India has been leading the world in awarding bachelor's degree equivalent science and engineering (S&E) degrees, followed closely by China.[6] The United States is a distant third with the largest percentage of S&D degrees awarded in the field of social sciences and behavioral sciences, a stark contrast to other S&E producing countries who tend to award engineering or physical, biological, mathematics, and statistics degrees (PBMS).[7]

Employees with engineering and PBMS degrees are exactly the type of skills needed to develop technology and operationalize decarbonization investments in the oil and gas industry.

For example, energy executives have noted that their companies lack employees with skills needed for the successful delivery of their decarbonization strategy, including technical/engineering (18 percent), carbon markets expertise (17 percent) or policy, regulation, or government relations expertise (16 percent).[8]

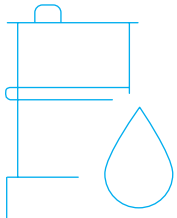
The onus is on oil and gas companies to make sure they get and retain the necessary talent by reviewing their recruiting and retention efforts. They also need to find ways to upskill or retrain their current workforce, which is what over 92 percent of energy companies plan on doing to address this climate skills gaps.[9]

New workplace dynamics: The oil and gas industry is regarded as a relatively staid, conservative one. But to successfully compete for talent these days, you may have to become more flexible and adapt to the new realities of the modern workforce. Spurred on by the COVID-19 pandemic, many companies permitted or accelerated remote and more flexible working arrangements for their employees whenever possible. This is a change that can help energy companies connect better with the values of coming generations.

Also, as the workforce diversifies, managers should seek to expand their understanding of how to work with people from different backgrounds. This may include acknowledging and embracing the increased importance of ESG and diversity, equity, and inclusion demographics (e.g., race, gender, sexual orientation) and values. This should be done at both the workforce and board levels.

You may also want to consider crafting a value proposition that resonates with younger employees and potential recruits. Keep in mind that money isn't everything, particularly for millennials; they tend to want challenging experiences that help grow their capabilities. What's more, different groups and different generations may require different value propositions and also have different learning styles and communication styles that should be taken into account.

For example, one oil and gas company found that it was losing many of the millennials it had recruited. They were using the same onboarding procedures that had been used successfully for decades, with dozens of written forms, endless pages of orientation materials, and hours of classroom sessions. They decided to switch to a more virtual, mobile and automated training process, which resulted in a much higher retention rate.[10]



Energy executives have noted that their companies lack employees with skills needed for the successful delivery of their decarbonization strategy, including

technical/ engineering

18%

carbon markets expertise

17%

or policy, regulation, or government relations expertise

16%[8]

[6] National Science Federation, Higher Education in Science and Engineering, (2018).

[7] National Science Federation, Higher Education in Science and Engineering, (2018)

[8] Eversheds Sutherland/KPMG, Climate change and the people factor (2021).

[9] Eversheds Sutherland/KPMG, Climate change and the people factor (2021).

[10] KPMG/Rigzone, When one crisis meets another: Focusing on talent for the long term (2015).

Tips for improving employee recruiting and retention

Here are several ideas oil and gas companies may want to run with to improve their recruiting efforts with potential employees:

- Ramp up (or reinstate) summer internship programs
- Sponsor (or increase your investments in) scholarships, prizes, fairs and afterschool programs that focus on STEM disciplines
- Organize business school conferences and job fairs
- Forge stronger relations with universities and other training institutes
- Promote interest in the STEM disciplines among high school (or younger) students with campaigns and programs designed to appeal to this audience

About the authors

Raad Alkadiri
Managing Director, Energy, Climate & Resources
Eurasia Group
E: alkadiri@eurasiagroup.net

Based in Washington, DC, Raad's work focuses on the nexus between politics, economics, climate, and the energy sector, as well as its effects on market behavior and investment risk. He works closely with clients to advise on capital-allocation options, risk-mitigation strategies, and policymaking. He also closely follows medium- and long-term geopolitical, energy, and climate trends, and their impact on the risk environment.

Regina Mayor
Global Head of Energy
KPMG International
E: rmayor@kpmg.com

Regina Mayor serves as KPMG's Global Head of Energy and Natural Resources. She is a recognized thought leader on the disruptive trends facing the various segments of the energy value chain — from the impact of millennial and baby boomers on gasoline consumption to the rapidly changing demands in the power generation segment. Regina brings over 25 years of experience delivering largescale business and technology changes to major energy companies around the world.

Stefano Moritsch
Global Geopolitics Lead
KPMG International
E: stefano.moritsch@kpmg.co.uk

Stefano leads KPMG's efforts, globally, to help companies and governments deal with today's geopolitical challenges. By connecting the dots between the macro political trends and their commercial implications in various sectors, Stefano hopes to help global businesses not only survive but thrive in geopolitical volatility. He can help identify the 'so what' of macro trends through strategic scenario planning, due diligence and geopolitical risk management.

Accelerating OT security for rapid risk reduction

Securing operational technology environments as they become increasingly digitized and connected

By: Serdar Cabuk, Jayne Goble, Ronald Heil, and Walter Risi

Oil and gas and other Industrial organizations are increasingly facing cyber threats not only to their information technology (IT) systems but to their operational technology (OT) environments as well. As OT becomes more connected, digitized and automated, so the potential for cyber attackers to break in and cause dangerous disruptions or overrides increases with it. Accidents and unintentional exposures have also caused major incidents.

That's why there should be an increasing focus on ensuring that OT environments are secure and subject to the same kind of good practice safeguards as in the IT domain. In just the past year, the roll-call of OT related incidents has grown. This includes a cyberattack on two German fuel and oil distributors[1] in late January 2022, disrupting operations and supply chain management, and an attack in 2021 that attempted to disrupt the water supply in Oldsmar, Florida[2] by gaining remote access to the system's control station and attempting to increase the levels of sodium hydroxide.

It's fair to say that events like these are probably just the tip of the iceberg. Whether the motive is financial — installing ransomware to extort large payments — or whether it's simply to cause disruption and danger to the performance and safety of critical infrastructure, we can expect to see more of this threat to industrial businesses in the future.

Certainly, attackers are becoming more professionalized and organized — and have the tools at their disposal to reach OT systems. IT malware and some OT malware are easily available on the dark web that can enable a hacker to get through the 'front door' and into an organization's systems. With the right skills and knowledge, attackers can then apply other malware to move laterally and reach the OT environment. Attackers will be doing their due diligence too — researching what software an organization's industrial control systems (ICS) run on and assessing what malware they may be susceptible to. In our experience, some software commonly used to run ICS have potentially severe vulnerabilities.

Against this backdrop, hardening OT security should be an absolute priority. And it is something that must be addressed at pace — cyber attackers won't wait to give organizations a decent chance to prepare first!

[1] BBC, Cyber-attack strikes German fuel supplies (2022)

[2] CNN, Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says (2021)

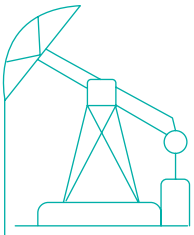
The convergence of OT and IT

It is also an imperative because OT is increasingly being converged with IT as new technologies are introduced to realize efficiencies, productivity gains and smarter operations. Whereas going back a decade or so, OT was segregated and inaccessible, now it is being connected to other systems. Standalone, non-connected OT simply doesn't meet today's performance and other needs. One analogy would be to the financial services industry: 10 —15 years ago, banks' mainframe systems were locked away, but they have had to re-engineer and digitize them to meet various modern needs including Open Banking and regulations such as PSD2, requiring new security protocols and protections.

Now, the convergence of OT and IT means that organizations must bridge the gap between the two environments' people, processes and systems to build a smarter, more secure network with high visibility to monitor and control both environments.

This brings us to an important point: to what extent is it useful anymore to distinguish OT from IT? As the two domains get closer to each other, a lot of OT *is* IT. After all, 80 percent of industrial plants have more servers and IT than an average bank. It is perhaps more useful — and will likely become more necessary in the future as operations become ever more digital — to think simply in terms of technology. Whether you look at OT or at IT, it's technology that they both come down to. The choice to keep them as separate environments will increasingly diminish.

This blending is becoming more visible in some interesting ways, such as the rise across industrial organizations of the Chief Technology Officer (CTO). In many senses this is still an emerging role — the responsibilities of a CTO vary from business to business in our experience. But as Boards place an ever-higher priority on digital transformation, it is CTOs to whom they are often looking to lead the change, comprising both IT and OT. The Chief Information Security Officer (CISO) remains a key role for security, and as OT security becomes a priority, it is extending to cover that too. In some ways, the CISO is moving from protecting IT (usually, the domain of the CIO) to protecting all the organization's technology (the domain of the CTO). Alternatively, some businesses have a specific OT CISO who reports into the overall CISO. The patterns vary — it's a developing picture — and it will be fascinating to see the direction of travel as this plays out.



Now, the convergence of OT and IT means that organizations must **bridge the gap** between the two environments' people, processes and systems to build a smarter, more secure network with high visibility to monitor and control both environments.

Top-down and bottom-up approaches

Whatever the case, clearly an essential component of securing OT is to have a top-down governance framework setting out roles, responsibilities and reporting lines, while not deferring a bottom-up detection and defense mechanism implementation. The definition of OT can be very broad, and it is found right across an organization's operations meaning that usually there is no single person with responsibility for all of it. So, coordinating efforts to address OT security is essential. This requires a clear governance structure and operating model. A strong mandate from the very top of the business is also a pre-requisite, to drive OT security as a strategic priority. That said, a bottom-up detection and defense approach must proceed almost in parallel, since threat actors won't wait until a governance framework is set. While the governance and operating model is instrumented, detection technologies (ideally, integrated into a security operations Cerisano (SOC)) should be implemented, response playbooks for common scenarios must be defined (e.g., ransomware) and basic cyber-hygiene measures should be taken care of.

Mature governance and operating model structures are geared towards delivering sustainable improvements over the longer term, helping also to future proof the organization as new technologies (and threats) emerge. But it's a simple fact that while organizations appreciate the value and importance of these top-down structural approaches, at the same time what we almost always get asked is: "What can I plug in today to make an immediate difference? What can I do to rapidly deliver OT risk reduction?"

These are valid questions — and they point to the fact that there are a number of bottom-up measures that can be taken alongside the top-down framework to make a fast and significant difference.

In many ways, it's a simple case of not reinventing the wheel: import best practices from IT security into OT (just as IT can import best practice from OT in other ways such as safety consciousness). So, there are three immediate areas that should be assessed and addressed:

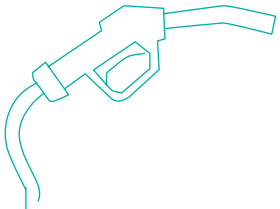
— Endpoint protection of OT assets

— Perimeter firewalls around OT assets

— Network segmentation, within OT and between OT/IT

Alongside this, organizations should implement OT network visibility in the early stages of their OT security journey. There are a number of technologies that allow monitoring of the OT network for either known threats or suspicious behavior. Ideally, these technologies should be integrated into the organization's existing monitoring and response framework (which typically would include a SOC and computer security incident response team).

Additionally, organizations need to strive for integrated asset management, at least for the most critical assets. Most businesses have a wide number of assets and several asset management systems, from IT's configuration management database to specific asset management systems the OT areas may have. The ability to manage these assets means firstly getting and then maintaining visibility of them — so this should be a priority. There are a number of tools available in the market that can instill asset visibility.



While the governance and operating model is instrumented, **detection technologies** (ideally, integrated into a security operations Cerisano (SOC)) should be implemented, response playbooks for common scenarios must be defined (e.g., ransomware) and basic cyber-hygiene measures should be taken care of.

Eight key questions

To understand the current state and then implement controls and processes that can make a speedy difference, we recommend asking yourself these eight questions:

1 Have you identified the cyber-related risks to which your control network is exposed and are you actively working to mitigate them?

An OT security risk assessment and cyber maturity assessment can provide you with a high-level view of what needs to be addressed at both the technical and governance levels.

2 Does an up-to-date inventory of your control network exist?

It's vital to know what needs protection within your production environment. Many commercial solutions for automatic asset detection are available which combine discovery and threat-detection capabilities.

3 What is the integration level between OT and the corporate network?

Ransomware commonly spreads through the network it attacks. Segmentation can limit its movement such as from the corporate network into OT and vice versa. Industrial intrusion detection systems (IDS) tools have features that can help with the modeling of a segregated network.

4 How is remote access to the network managed?

Secure remote access is a vital topic when it comes to maintaining and repairing assets from a distance, especially in the COVID and post-COVID world. Common remote access types include Remote Desktop Protocol (RDP) and virtual private network (VPN). Secure remote access software is now commonly available on the market and should be considered.

5 Is a solid back-up mechanism in place and consistently tested for security?

If OT assets are infiltrated, the only options may be to either pay whatever ransom is being requested (and, increasingly, it is becoming more common for organizations to take out ransomware insurance) or to restore a backup. Backups can be complex and the medium where they are stored is critical to prevent them becoming infected with malware too.

6 What methods are used to apply security patches?

Patch management is essential — and can be difficult if an asset is in use 24/7. Critical assets must be regularly updated. However, for assets with low criticality, it may be possible to apply a patch in the next scheduled maintenance interval.

7 What are your current anti-malware solutions?

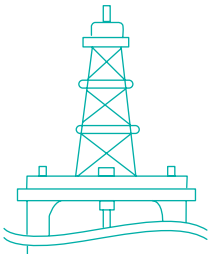
Early detection is crucial — such as through IDS tools. Detection tools should be connected to a Security Incident and Event Management (SIEM) system which should log multiple sources including firewalls, assets and remote access tools so that it can alert teams to a possible attack.

8 Do you have a zero trust mindset?

Many organizations consider OT to be a walled garden from IT, and anything behind that wall is trusted. This model has proven to be flawed — we can go back as far as the Stuxnet attack of 2010 when a truly air-gapped system was breached through a compromised vendor. Instead, organizations need to start adopting a zero trust mindset and architecture that doesn't assume anything about trust levels, but entails gathering additional context within the network traffic and then making decisions on what to allow or deny based on this information. While having its roots in IT, zero trust can be adapted for OT.

Leveraging emerging technologies

Once a solid security foundation is in place, there is also a role for AI technologies to play. A robust security posture calls for "shifting security to the left", that is, expanding preventative and detection capabilities, averting threats before they become damaging incidents. This requires asset identification and characterization, early-stage threat detection — and, where appropriate, autonomous response. AI technologies have been developed that can provide a way for organizations to increase these capabilities with layered applications of machine learning.



A robust security posture calls for **"shifting security to the left",** that is, expanding preventative and detection capabilities, averting threats before they become damaging incidents.

By passively observing and dynamically understanding the contextual behavior of all assets, self-learning AI provides a continually updated asset inventory that allows organizations to gain full visibility into their IT, OT and IT-OT converged environments. Further, self-learning AI's understanding of the nuances that underpin unusual behavior allows it to identify threatening activity at its earliest stages, presenting the threats to be dealt with before they can escalate into a crisis.

Accelerating responses through machine learning is also of particular use when defending against ransomware. Companies must take decisive action in the moment to halt the propagation — and machine learning enables them to assess the threat faster.

For ransomware threatening industrial environments, self-learning AI's abilities to respond autonomously — mathematically calculating the most precise way to neutralize a threat without affecting normal operations — is particularly valuable, as it can disrupt threats in IT long before they have the chance to spread into OT systems.

Getting the people and teams approach right

This brings us back again to the question of the boundaries between IT and OT — in many senses the challenge for organizations is to keep prudent security segregations between the two while at the same operationally converging them.

Key to the success of this balancing act is people. Both functions should learn from each other as they come closer together.

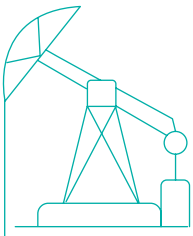
For example, one of the hallmarks that is absolutely baked into people working within OT environments is the safety and challenge culture. These attitudes should be adopted within IT. Now that their work is more directly integrated with manufacturing or production systems — and the humans physically operating them — IT administrators need to recognize the elevated stakes associated with cybersecurity. The resulting cultural change within IT should better prepare IT processes and workflows for convergence.

On the other hand, OT processes and workflows should be adapted to fit a more regular schedule of updates. This approach is necessary to support cybersecurity in a converged environment that contains more connected devices and potential vulnerabilities. IT administrators are acquainted with this approach and their expertise should be utilized when designing new OT processes, systems and capabilities to support convergence.

In short, there are things that people in each team can take from each other and teach each other. Creating a common culture and sense of team — underlining the fact that everyone ultimately shares the same objectives — is key to success. There is often a lack of collaboration between IT and OT teams, which leads to weak, uncoordinated security programs, as well as poor funding and low risk awareness. This needs to be overcome through a collaborative mindset that recognizes today's increasing convergence of technology and operations.

At the same time, there may be scope to combine teams or aspects of teams for greater clarity and simplicity. For example, there may be teams managing firewalls on both sides of the OT/IT fence — removing duplication of effort here makes business sense and could also produce cost savings.

It may be some way off in the future, but as tasks are increasingly carried out remotely — even by OT staff who no longer need to be physically on-site for routine activities — it would not be surprising if, eventually, IT and OT teams became one. Just as the disciplines of IT and OT themselves may become subsumed into the one concept of technology.



Creating a common culture and sense of team — underlining the fact that everyone ultimately shares the same objectives — is **key to success.**

Four takeaways

Managing OT in today's aggressive cyberattack environment is challenging. It demands rapid action to reduce the risks faced and find approaches that recognize OT's increasing convergence with IT.

But it can be done — and here are some priority tips to check against to measure your progress.

1 Take best practices from IT
Take the processes that are common in the IT environment and apply them to OT. For example, patch management can be carried across — it's not something that has to be reinvented.

2 Consolidate and combine
Reduce the number of products and asset management approaches in use where you can. Simplifying makes the task more manageable. Combine groups across OT and IT where they are carrying out the same tasks where appropriate too. Of course, you need to make sure you are not harming service quality and standards when doing so.

3 Think strategically — but also like an attacker
Focus on your long-term program but don't lose sight of the here and now. What are your most valuable OT assets in a cyber criminal's eyes and how are they likely to try to reach them?

4 Don't 'boil the ocean'
Focus on your priority assets and protect those. If half of your asset base is already behind a segregated network, focus on the other half. Don't create solutions for things that are already up to standard — concentrate on vulnerabilities and threats.

How KPMG firms can help

KPMG firms have extensive experience of helping oil and gas and industrial organizations rapidly reduce the risks in their OT. We can advise on and implement industry best practices, effective standardization and available market solutions. Through our wide range of industry relationships and work, we 'speak both languages' — fluent in both OT and IT! We can help you bridge the gap between the two as well as create engagement at all levels of the organization — from the boardroom to the operational control room.

We'd be delighted to talk to you about any aspect of accelerating your OT — keeping it modernized, secure and safe, and making it fit both for the present and the future.

About the authors

Dr Serdar Cabuk
Partner, Cyber and Technology Risk
KPMG in the UK
E: serdar.cabuk@kpmg.co.uk

Serdar is a partner in the Corporates Consulting practice at KPMG focusing on cyber and tech transformation in energy and consumer sectors. Previously he was the managing partner for a big four cyber practice in the Nordics and IBM's European leader for cyber risk services before that. He brings 20 years' of cyber, cloud and digital transformation experience also having led major response and recovery operations with global energy firms during several major incidents.

Jayne Goble
Director, Cyber Security
KPMG in the UK
E: jayne.goble@kpmg.co.uk

Jayne Goble, PhD leads KPMG's UK OT and IoT team and has over fifteen years' experience working with a range of global clients to oversee and deliver a variety of capital projects, ranging from responding to critical security failures of national infrastructure, to deployment of interception and intelligence platforms.

Ronald Heil
Global Cyber Security Leader for Energy and Natural Resources, KPMG International and Partner, KPMG in the Netherlands
E: heil.ronald@kpmg.nl

Ronald is a partner at KPMG in The Netherlands and is the Global Cyber Lead for the Energy and Natural Resources sector for KPMG International. He has extensive experience helping international companies connect their products and devices to the Internet of Things and providing information security and ICS/SCADA advice.

Walter Risi
Global IoT Lead and Partner
KPMG Argentina
E: wrisi@kpmg.com.ar

Walter is the Global IOT Lead and the Technology and Cyber Security Consulting leader at KPMG in Argentina. During his 20-year career, he has assisted companies in the application of technology management best practices, cybersecurity, transformation and software engineering. He's led both technology consulting teams and software development factories and is currently focused on the convergence of agility and cybersecurity in Digital Transformation.

Bringing cyber process hazard analysis to the digital era

Extending process hazard analysis to cover cyber risks

By: Hossain Alshedoki and Tim Johnson

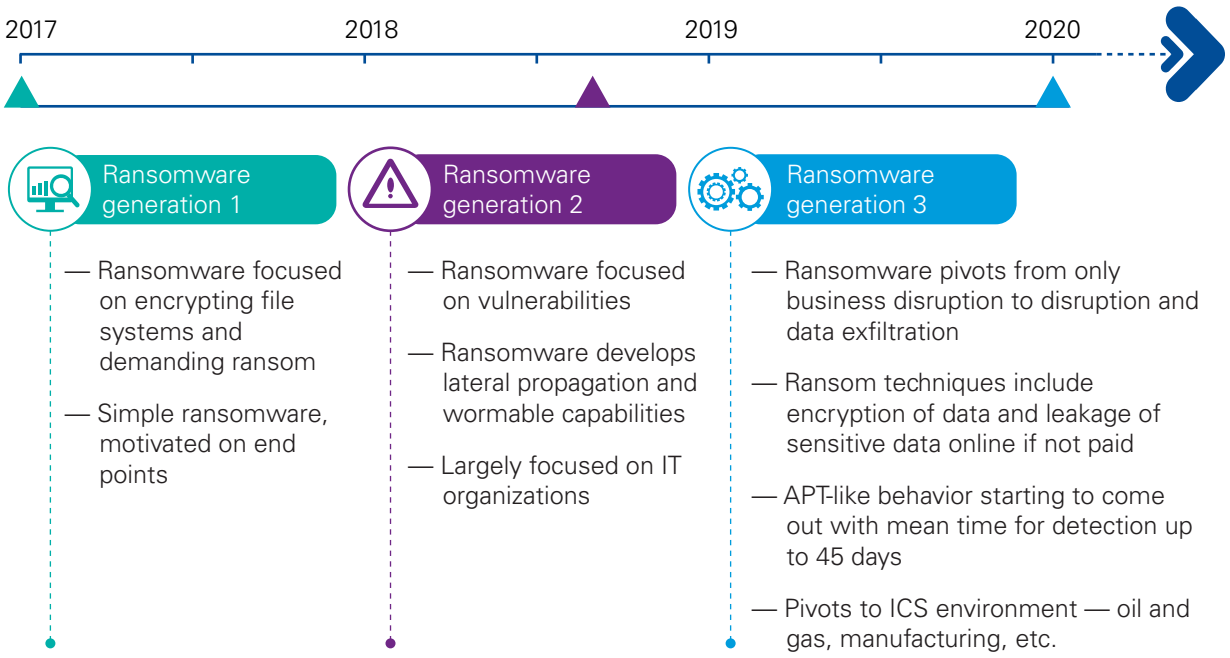
Process hazard analysis (PHA) is an established feature of the oil and gas and industrial plant world, performing reviews and remediations over hardware in the operations that processes depend on. Based on the OHSA 1910.119 methodology, PHA relies on 14 inter-related elements to create a comprehensive program to prevent the release of hazardous materials.[1]

But as the hardware within industrial businesses' networks becomes increasingly enabled by technology, with process control components communicating with each other in an Industrial Control System (ICS)/Operational Technology (OT) domain, so new risks arise that demand new levels of PHA. Process control components are no longer standalone items that exist in isolation, shut off from other parts of the ICS domain or information technology (IT) network. ICS/OT requirements to interact with IT is producing increasing convergence, expanding paths and pivot points through critical process control processes. There is a growing intersection between safety systems and process control systems resulting in new attack vectors that can be exploited by cyber attackers.

This issue is becoming all too real. Incidents of ransomware attacks on OT networks have been multiplying, soaring five-fold from 2018 to 2020. Out of these, manufacturing entities comprised over one-third of confirmed ransomware attacks on industrial organizations, followed by utilities, which made up 10 percent.[2] The estimated global cost of these ransomware attacks has skyrocketed and has been predicted to reach USD20 billion in 2021— up from USD325 million in 2015.[3] Operational disruption due to ransomware in OT environments has seen a 23-fold increase. In 2020, there was a 32 percent increase in ransomware attacks against energy and utilities organizations.[4]

Over time, ransomware attacks have become more sophisticated and have changed to achieve their ends by different methods. Additionally, these kinds of attacks have increasingly targeted ICS environments like oil and gas and manufacturing.

Ransomware on the rise[5]



[1] US Department of Labor, Occupational Safety and Health Administration, 1910.119 — Process safety management of highly hazardous chemicals

[2] Ransomware in ICS Environments, Dragos, December 2020.

[3] Global ransomware damage costs predicted to exceed $265 billion by 2031, Cybersecurity Ventures, June 3, 2021.

[4] Claroty Biannual ICS Risk & Vulnerability Report: 1h 2020, Claroty, 2020.

[5] Securing a hyperconnected world, KPMG International, 2021.

A rising threat landscape

Ransomware attacks are just one feature of a complex and increasingly aggressive threat landscape that organizations should protect themselves against. This includes:

Evolving threat actors

Cybercriminals are adapting, diversifying and behaving more like state actors. Criminal operations are changing their tactics to reduce risks of detection and increase disruptions. They are attempting to maximize the return on their effort in several ways such as: shifting away from partnerships to operating within close-knit syndicates; taking advantage of the increased availability of ICS information to launch attacks; increasing the precision of targeting by using legitimate documents to identify likely victims before delivering malware; or selling and buying direct access to networks for ransomware delivery rather than carrying out advanced intrusions.

Targeted ransomware

There is a complex range of motives at play in targeted ransomware attacks. While the motivation behind an attack may appear to be financial, there may be hybrid motives at work — a combination of financial, ideological and/or political drivers. Regardless, such attacks have the potential to impact the availability of ICS/OT. While the ransomware threat remains, organizations should ensure they take adequate measures to prepare, prevent, detect, respond, and contain a corporation-wide ransomware attack.

Supply chain threats

Improved ecosystem hygiene is pushing threats to the supply chain, turning friends into enemies. The global interconnectedness of business, the wider adoption of traditional industry cyberthreat countermeasures and improvements to basic cyber security hygiene appear to be pushing cyberthreat actors to seek new avenues to compromise organizations, such as targeting their supply chains — including those for software, hardware and the cloud.

Life after meltdown

Vulnerabilities in ICS/OT infrastructure demand tuned/targeted solutions to prevent impact to availability. The discovery of vulnerabilities in proprietary process control hardware such as programmable logic controllers (PLCs), in recent years combined with the use of commercial software and hardware used for human machine interfaces (HMIs), Engineering Workstations, and ICS supporting systems such as Historians, have an impact on system availability increasing the risk to organizations which could lead to loss of life.

Compromising geopolitics

As new threats emerge from disinformation and technology evolution, global businesses may find themselves in the crosshairs as geopolitical tensions persist. Cyberthreat actors may not only sustain current levels of activity but also take advantage of new capabilities as new technologies enable more sophisticated tactics, techniques and procedures (TTPs) which are focused on ICS/OT environments.[6]

[6] Security magazine, Five factors influencing the cyber security threat landscape (2019)

Strengthening defenses through cyber PHA

As a result of these factors, expansion of traditional PHA is required to protect process control performed in the ICS/OT domain. This need is made more acute because safety system communication is becoming integrated into the ICS/OT domain as these systems become more digitized and connected. If the interconnected safety system is compromised, the ability to control a runaway process is compromised — potentially leading to environmental and operational hazards, and even loss of life. And with control and safety systems becoming more converged with IT systems, a cyber breach into IT could then more easily spread into the ICS/OT domain as well.

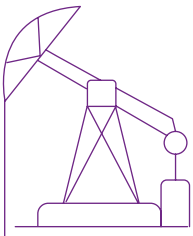
That is why additional Cyber PHA is needed, to address the cyber risks and threats that now characterize today's industrial landscape. Welcome to cyber PHA.

In an ideal world, the first step is to ensure that your ICS/OT domain is cyber resilient through network segmentation. This involves segmentation of the network into zones and conduits, and a distinct boundary between IT and ICS/OT domains. This is the premise of IEC 62443, a series of standards to guide on secure ICS/OT. It covers general guidance, policy and procedures, system technology and design, as well as component requirements. In any event, regardless of whether formal network segmentation is in place, there should be a focus on bolstering cyber resiliency such that operations can continue to function even if a threat actor has penetrated the perimeter of a network.

A cyber PHA can help identify, verify, and design ICS/OT domain boundaries. The Cyber PHA is a safety-oriented methodology to identify and assess cyber risk for ICS/OT domains and safety instrumented systems (SIS). It usually follows a methodology similar to a HAZOP (hazard and operability study) but adapted for cyber specifically — to be known as CHAZOP.

A cyber PHA is typically performed in phases, is scalable, and can be applied to individual systems, or entire facilities or enterprises. There are six key phases:

1. The site personnel and threat assessor - the Hazard and Operability team (HAZOP) should align and agree on the focus area that will be assessed.
2. Gather information about the OT components with the OT network and the SIS, and its connections to identify vulnerabilities.
3. Analyze the data and document potential vulnerabilities that may be exploited during a cyber event.
4. Conduct a cyber PHA workshop where information is gathered, analyzed and integrated with threat scenarios to develop a complete picture of risks.
5. Once the cyber PHA is completed, a broad report is produced showing the risks to the ICS/OT domains and SIS, and a plan to mitigate risks to the organization's acceptable level.
6. An effective remediation plan includes a prioritized list of actions, budgetary estimates, schedule, and resource requirements, which together can provide appropriate levels of resiliency.



The Cyber PHA is a **safety-oriented methodology** to identify and assess cyber risk for ICS/OT domains and safety instrumented systems (SIS).

An ideal scenario would see a cyber PHA carried out as a follow-on shortly after a traditional PHA, building on its findings to identify and address cyber issues.

The outcome of the hazard and risk analysis should identify potential hazards and vulnerabilities while providing actionable risk themes facilitating practical recommendations for implementation. Although the cyber security threat landscape is continually changing, there are general classifications of potential threat agents or sources for an organization to consider:

1 External attack — technical

2 Internal attack — non-technical

3 Internal misuse and abuse

4 Unauthorized access

5 Compromise of information (Logic Mod)

6 System malfunction

7 Process interruption

8 Safety-system interruption

9 Human error

10 Unforeseen effect of changes

A detailed cyber security roadmap can be developed and broken into summarized key quick wins, multiple short-term remediations, and long-term strategic alignments to align OT and IT security programs.

The benefits of cyber PHA

There are multiple potential benefits to be gained from conducting a cyber PHA. Most obviously, ensuring system availability by removing system cyber risk. But a cyber PHA can also benefit an organization's broader business practices. Applying a cyber PHA methodology documents an organization's business processes and requires the creation of ICS/OT aligned information security policies, procedures, standards and controls with organization objectives.

— Clearly defined articulation of the information security strategy based on organization and business unit objectives.

— Engineering knowledge defined and aligned security controls based on risk and business objectives.

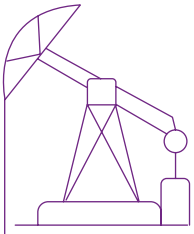
— Confident effective staffing resulting from established roles and responsibilities.

— Interconnected system cause and impact identification facilitating vulnerability and risk management.

— Targeted and prioritized cyber response and incident management.

— SecOps defined metrics, reporting, and technology requirements to help meet business objectives

A cyber PHA also gives organizations the visibility from a cyber point of view that can be leveraged to expedite ICS/OT and IT convergence, thus helping achieve what is rapidly becoming a key strategic aim for many businesses. ICS/OT and IT convergence has the potential to create and streamline the exchange of data facilitating business operations. But cyber risks are hindering this IT/OT convergence — so carrying out a rigorous cyber PHA that helps identify operational risk, required mitigations, and residual risk, can provide the data to give management confidence in pursuing the convergence agenda.



The Cyber PHA is a **safety-oriented methodology** to identify and assess cyber risk for ICS/OT domains and safety instrumented systems (SIS).

Cyber PHA on the regulatory radar

But cyber PHA is not only a matter of potential business benefits and best practice — it is also coming onto the regulatory radar and may, in varying shapes and forms, become mandatory in the coming years.

Indeed, in Saudi Arabia the National Cyber Authority has already launched a new regulatory framework for Operational Technology which includes a specific revision that oil and gas and other critical infrastructure entities should conduct formal process hazard analysis which should include, as a minimum, qualitative analysis of cyber risks.[7]

If this becomes adopted into the framework, it will effectively be making cyber PHA a mandatory regulatory requirement — and that could take effect later on this year.

[7] National Cybersecurity Authority, Operational Technology Cybersecurity Controls (2022)

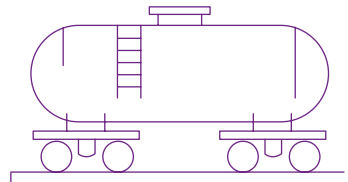
Meanwhile in the US, new measures have been introduced by the Department of Homeland Security (DHS) in the wake of last year's Gas Pipeline cyberattack which disrupted the flow of gasoline and jet and diesel fuel along the East Coast. The DHS issued two Transportation Security Administration (TSA) Security Directives that feature a number of measures that owners and operators of critical oil and gas pipelines must implement.[8] The first directive features guidance around cyber security incident reporting, the appointment of an organizational cyber coordinator, and gap assessment. The second directive is the one that really has teeth, requiring specific mitigation measures, a formal cyber security contingency and response plan, and an annual review of cyber security architecture.

These requirements, that also include the need to carry out an analysis of network traffic in OT systems, can almost be regarded as 'cyber PHA-lite'. What DHS is really asking of these companies is to quickly gain an appreciation of the unique systemwide cyber security components and communications, as well as the interdependencies of IT and OT and the protections that are, or are not, in place.

Elsewhere, the International Electrotechnical Commission (IEC) 61511 Functional Safety standard now requires a SIS security risk assessment. The updated report summarizes the risk assessment procedure called cyber PHA. The link to PHA here is a step in the risk assessment to firstly, review the output of the PHA to identify worst-case health, safety, security, and environment (HSSE) consequences for the asset and secondly, to identify any hazard scenarios.

Another example comes from the User Association of Automation Technology in Process Industries (NAMUR), who have already published a worksheet (NA 163) titled "Security assessment of SIS." Here, a cyber PHA methodology can be used to assess the risks linked to identified cyber security escalation factors and recommended mitigations to reduce risks to a certain level. By creating a bridge between PHA methods and cyber security risk assessment methods, safety systems become more robust against cyber security attacks.

In short, the direction of travel is towards more formalized regulatory requirements around the cyber-related aspects of operational safety — the very area that cyber PHA is designed for. At present, there may be few jurisdictions who are explicitly moving in a cyber PHA regulatory direction, but the number may quickly grow. In addition, due to the global and inter-connected nature of the energy and natural resources industry, requirements in one jurisdiction are likely to be felt elsewhere by others. If a supermajor operating in Saudi Arabia, for example, becomes required to conduct a cyber PHA, then it may ask the partner organizations it works with in other parts of the world to carry one out too. A rising tide lifts all boats after all!



The direction of travel is towards more
formalized regulatory requirements
around the cyber-related aspects of operational safety — the very area that cyber PHA is designed for.

[8] Department of Homeland Security, DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators (2021)

How KPMG firms can help

KPMG firms have already helped a number of clients by leading and performing a cyber PHA. Our multidisciplinary teams with extensive sector experience work closely with CISOs, CTOs and Risk teams at a corporate level, as well as Plant Managers, Operations, and other ICS/OT domain key stakeholders.

For example, we helped one firm's client who needed to standardize its processes across a heterogenous environment of systems across multiple vendors, bringing all to the same operating security level. Following a gap assessment and stakeholder interviews, we conducted an analysis based on cyber PHA as part of the response alongside other technical security assessments, the design of zones and conduits for two different types of ICS network, and the design of monitoring dashboards to better understand risk exposure.

If you would like to discuss any aspect of a cyber PHA and how it relates to your broader IT and OT security posture, please don't hesitate to get in touch. After all, the signs are that cyber PHA requirements are coming down the pipe and may soon be expected of increasing numbers of industrial players.

About the authors

Hossain Alshedoki
IT/OT Cyber Security & Data Privacy Energy and Natural Resources Lead, KPMG in Saudi Arabia
E: halshedoki@kpmg.com

Hossain is an IT/OT Cyber Security leader, specializing in leading teams within a converged business and operational technology environment. Hossain provides intermediary client stakeholder guidance from technical design to board level in areas that utilizes Industrial Controls Systems (ICS), Big Data integration, SCADA, DCS, SIS, IoT and IIoT. Hossain comes from an engineering background with a Cyber Security focus on technical critical infrastructure and consulting in different sectors have been instrumental in the firm's growth and success within the Cyber Security space and a major contributor to the Kingdom of Saudi Arabia vision 2030 on a national level.

Tim Johnson
Director Advisory, Cyber Security Services KPMG in the US
E: timjohnson@kpmg.com

Tim is a seasoned cyber security leader with significant experience leading some of the world's most influential organizations through cyber security transformation of Industrial Control System (ICS) technology and governance. During Tim's career in critical infrastructure and consulting, he has built a reputation for safeguarding ICS availability while implementing cyber security and governance requirements across various industries.

Safeguard your digital environments from all angles

Five steps to beginning the ‘zero trust’ journey

By: Ronald Heil, Manuel Kanagasuntherie, Dani Michaux and Brad Raiford

If oil and gas companies weren't already on notice, recent events should have hammered home the message that they need to shore up cyber defense protections of their digital networks. As information technology, operations technology and IoT departments — and the hardware and software systems they access — continue to converge, the need for digital security becomes even more critical as an exposure in any one area can spill over to others.

In a similar fashion, oil and gas companies have a complex ecosystem of partners, suppliers and service providers, many of whom have connected computer networks. If any one of these third parties experience a cyber breach, it can endanger the systems of the oil or gas company with whom they're doing business.[1]

What's more, cyber criminals are continuously evolving, becoming more creative and devious, and wreaking more havoc on businesses, consumers and governments. And oil and gas companies are particularly susceptible.

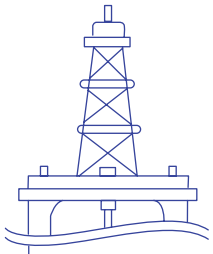
Their headquarters, operations and power plants, production sites, gathering systems, refineries, chemicals processing sites, and midstream pipelines, as well as their wider partner, supplier and services interconnections, are often spread out over wide geographic areas around the globe, leaving them precariously exposed. And because many locations and sites involve more than one firm — for example, one company owns an oil platform but another operates it — the lines for responsibility for security get blurred.

What's more, their digital networks and physical equipment are frequently in need of updating for cyber security purposes; while they were built to last and operate for a long time, the downside is that its cyber protection is outdated. And in addition to the usual "in-it for the money" cybercriminals, the oil and gas industry has to contend with environmental "zealots" who are not above trying to sabotage business operations by hacking into computer systems.[2]

That's why it's high time for the oil and gas industry to likewise evolve and take the next step forward in protecting their business, employees and customers by adopting a "zero trust" approach. The zero trust approach enables you to set up adaptive and continuous protection for users, data and assets that proactively manages risk through key enforcement points. This allows you to potentially continue operating your business even while under attack.

So, for example, the zero trust approach could have significantly mitigated damages in the Colonial Pipeline incident. Colonial could have simply walled off the part of their operations infected with the "ransomware" and continued to operate while simultaneously fighting the cybercriminals; but since it couldn't be certain that the "infection" wouldn't spread, it opted to essentially shut down its entire business operations.[3]

Although the zero trust concept has been around for quite some time, only recently has the technology caught up to it and made it feasible. In other words, since zero trust typically relies on cloud/hybrid cloud adoption, identity, and network modernization, only recently has it become conducive for companies to realize the full potential value of zero trust. In this report, we will explore the zero trust journey, what it is, how it works, and how to design and implement a program.



More companies using zero trust

80%

of new digital business applications opened up to ecosystem partners will be accessed through zero trust network access by 2022

Source: Gartner

[1] Shell, Third-party cyber security incident impacts Shell (3/16/21).

[2] The Intercept, Dakota Access Pipeline Activists Face 110 Years in Prison (2019).

[3] The Hill, Embracing zero trust is the right answer to the colonial-pipeline-hack (2021); Cyolo, 4 Cybersecurity breaches in Q2 2021 & how to prevent them from reoccurring (July 7, 2021).

Cyber crime is big and growing

Opportunities for cyber breaches have expanded exponentially over the past several years. New, more mobile working arrangements, innovative cloud technology, and increased business dealings with vendors and other third parties have created a more porous perimeter, increasing the attack surface and exposing vulnerabilities (i.e., more opportunities) for cybercriminal attacks. In the face of these developments, the traditional "cyber security perimeter" defense [See Exhibit A] has become far less effective, enabling cyber criminals and other "bad actors" to exploit weaknesses and holes with more frequency and do far more damage.

By 2025, global cybercrime damage is expected to reach $10.5 trillion annually.[4] And in the US in 2020, the average data breach cost organizations $8.64 million.[5] Aside from a purely dollars-and-cents damage, these breaches can also have worker safety as well as environmental and safety implications on the surrounding communities. They can also jeopardize a company's brand and reputation, undermining its customers' trust in the reliability of the company and the safety of their private data. In addition, these breaches also expose the company to litigation and regulatory penalties.

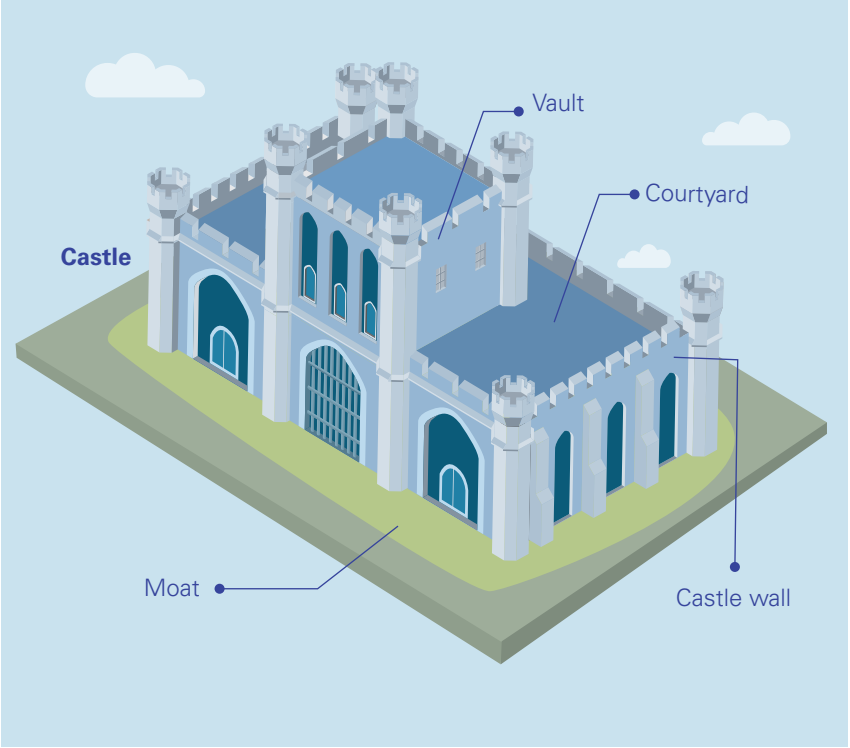
For oil and gas companies, the stakes can be even higher. Considering the essential role they play both nationally and globally, and depending on the nature and severity of a breach, a company's ability to survive as an ongoing entity can be called into question.

That's why more companies are taking a zero trust approach to shore up their cyber defenses.

Even the US government has strongly endorsed the zero trust concept. The Biden Administration recently rolled out a zero trust mandate for federal agencies, and the fallout is expected to ultimately filter down to private industry.[6]

Exhibit A: Outdated castle cyber defense setup

Below is an example of the traditional "castle-moat" security defense system



[4] Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (November 13, 2020).

[5] Statista, Average organizational cost to a business in the United States after a data breach from 2006 to 2020 (November 15, 2021).

[6] The White House, Executive order on improving the nation's cybersecurity (May 12, 2021); OMB Memo M-22-09, Moving the US Government Toward Zero Trust Cybersecurity Principles (Jan. 26, 2022); mimecast: Cyber Resilient Insights, Biden Aims to Drive Zero-Trust Architecture Nationwide (Jan. 20, 2022).

Zero trust basics: The perimeter-less border

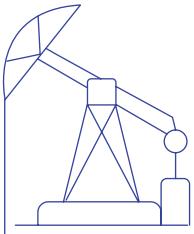
With zero trust, you establish what is often referred to as a "perimeter-less" defense system[7] based on the principal of never trusting and always verifying individuals and devices, regardless of whether they are inside or outside of the organization. Before access to a system or app is granted, the person or device seeking access must be identified, assessed, verified and authorized. And this authentication process takes place each and every step of the way. However, from the user's perspective, the process is quick, easy and seamless — unless issues are detected.

This stands in marked contrast to the traditional "castle and moat" cyber security defense, where once a person (or device) manages to cross the moat and enter or breach the front door or wall of the castle, there's relatively easy access to the "crown jewels." That approach is no longer enough in this new world environment where cyber criminals are more cunning then ever and more employees — as well as vendors, contractors, suppliers and even business partners — need immediate access to data from enterprise apps and systems located anywhere in the world and from any device via the internet.

With zero trust, whomever (or whatever) attempts to access your systems — along with the device they're using — is identified, assessed, authenticated and authorized in light of the system they are trying to access, and that session is continuously monitored. And when they seek to access another system, the process is done all over again.

So using the castle analogy once individuals manage to cross the moat, they would have to go through a reauthorization process to get through the front door. And the same thing would occur whenever they attempted to move to a different part of the castle. In some cases, depending on the individual's approved authorization, he or she would only be allowed to go directly to a particular room; in fact, the individual wouldn't even have visibility into any other room in the castle. (Think hotel or building elevator that only takes you to a particular floor.)

Taking it one step further, with the right zero trust model that is implemented properly, an individual would only be able to go directly to the bathroom off of a particular guest bedroom (assuming the bathroom was the intended destination). And with today's powerful computer capabilities, the identification/authentication/authorization process would occur seamlessly and nearly instantaneously (or at least quickly).



With zero trust, whomever (or whatever) attempts to access your systems — along with the device they're using — is **identified, assessed, authenticated and authorized** in light of the system they are trying to access, and that session is continuously monitored.

[7] Technically, a zero trust process is not truly perimeter-less. Zero trust does not rely on the traditional "moat" style perimeter, but instead replaces it with hundreds and thousands of smaller perimeters, each one wrapping around every user, device, connection and so on.

Principles of zero trust

Principles are the lynchpin to zero trust. All solutions should embrace multiple of them to align with the overall enterprise vision of zero trust.

01 **"Perimeter-less" design** — Connecting from a particular network must not determine which services you can access

02 **Context-aware** — Access to services is granted based on what we know about you and your device

03 **Dynamic access controls** — All access to services must be authenticated, authorized, and encrypted

04 **Continuous assessment** — Shifts away from one-time binary decisions

05 **Fine-grained segmentation** — Uses granular policies and controls to segment network and access

06 **Active risk analysis** — Discovers, monitors, assesses and prioritizes risk, both reactively and proactively

07 **Establish and review trust** — Performs risk and trust assessments early and often

08 **Real-time monitoring** — Continuous feedback and anomaly detection

Key potential benefits of zero trust

Key potential benefits of a zero trust approach are that (1) it prevents bad actors from getting authorized and then accessing your system and (2) in the event of an initial breach, your company would be able to detect and isolate the intruding person, device or "bug" and turn off its access to the system, not allowing it to pivot or escalate the attack.

For example, one of the world's leading shipping companies, was brought to a standstill by cybercriminals who installed ransomware on a local office server in the Ukraine. The virus then spread throughout the company's entire global network, causing an estimated $250–$300 million in damages. But a zero trust approach, with its multiple reauthentication security and continuous session monitoring process, could have limited the damage to the Ukraine and not caused a company-wide shut down.[8]

Similarly, in 2021, a state-owned oil company was the victim of a cyber attack. The perpetrator accessed confidential data through the system of a third-party contractor with whom the company did business. Although its business operations weren't interrupted, the cybercriminal demanded $50 million from the company or threatened to sell the information to any other party for $5 million. Had the company been operating a zero trust strategy, it's unlikely its systems would have been breached.[9]

[8] Forbes, Why manufacturing supply chains need zero trust. (2019)

[9] Flashpoint, Saudi Aramco Data Breach Highlights Risks to Oil and Gas Industry (2021).

There are a host of other potential benefits to be gained by a zero trust approach. For example, it can:

Improve network visibility, breach detection, and risk vulnerability management.

Break down interdepartmental siloes as IT, HR, marketing, operations compliance and others need to work together to get it right.

Reduced both capital and operational costs in the long-term.

Enables and supports digital business transformation and improved business agility.

KPMG helps global retailer implement zero trust program

Due to the COVID-19 pandemic, a global retail client's entire workforce started working remotely from home and connecting to their network through virtual private network (VPN). The employees were using a cloud-based collaboration platform to work with their teams. In addition, the company started leveraging more cloud-based applications and platforms to support the business.

This led to a significant increase in VPN traffic, poor network performance, and a poor user experience. What's more, the increased work from outside the office from a variety of devices increased the potential for a cyber breach.

Client solution: KPMG helped the client implement a zero trust process that enabled it to secure the new cloud environments by shifting away from one-time binary access decisions to contextual, risk and trust-based decisions. This allowed remote users to access their data and resources securely over the Internet while also reducing the amount of VPN traffic and providing a better user experience.

Getting started on your zero trust journey

A critical element in designing and implementing a zero trust architecture is understanding that it may represent a cultural change and challenge to your organization. Therefore, you will need commitment from senior management to help overcome resistance to it.

And while the CIO and the cybersecurity department may lead the effort, you also need the buy-in and cooperation of the entire organization — including information technology, operational technology, IOT, HR, compliance and regulatory, and sales and marketing — to get it right.

The zero trust security architecture must integrate with the organization's security and IT environments to enable speed and agility, improve incident response, and support policy accuracy and the delegation of responsibilities. At the same time, the authentication and reauthentication measures cannot unduly burden the normal operations of the business, particularly in terms of wasted time.

Here are some key steps to help you get started on your journey:

1

Determine what you're trying to achieve:

Don't start with the solution. Determine what needs improvement and which zero trust components make sense. Also, keep in mind that the zero trust model doesn't have to be implemented all at once; it can be phased in and tailored to your organization's level of maturity.

Identify and prioritize which data and assets are most valuable:

Collect as much information as possible about the current state of assets, network infrastructure and communications. Also, classify the level of "sensitivity" of each asset, for example, the customer database, source codes, confidential or proprietary information (e.g., business process), the HR portal. Which are "restricted," "highly restricted," and so on.

2

3

Map data flows across your network.

This step is a primary reason why you need the input and cooperation of multiple departments and not just cybersecurity and IT; the zero trust approach impacts everyone. The data flows include:

— North-South traffic, such as from a front-end web portal to back-end servers.

— East-West traffic, such as purchase information to fulfillment and accounting systems within the corporate network.

Group assets with similar functionalities and sensitivity levels into the same micro-segment.

This will help you determine when and where authentication and reauthentication may be needed, so you can

4

— Deploy a segmentation gateway: This can be virtual or physical and will enable you to achieve control over each segment.

— Define a "least privilege" access policy to each of these assets, whereby access to services is granted based on context and the risk profile of users and devices (e.g., a public device, based in a suspicious location or on company premises), and all access must be authenticated, authorized, and encrypted.

5

Select the right technologies and services to support zero trust:

The cybersecurity team will be instrumental in this decision, but will certainly need input from other departments, including finance. It's critical to build in flexibility that will be needed to adapt to everchanging risks and the ability to conduct real-time monitoring and continuous assessment and anomaly detection.

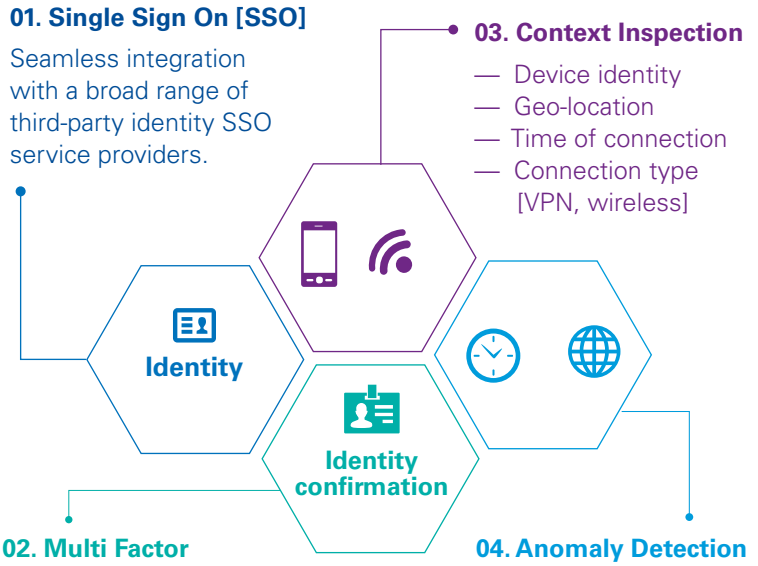
— When making the presentation to senior management or other decision makers, be prepared with a final estimate of resources needed as well as the proposed timing for implementation.

If done correctly, a zero trust approach doesn't just block cyber criminals and bad actors from doing things they shouldn't be able to do; it enables people to do their jobs better — with less friction and a higher degree of security"

Brad Raiford
Director, Cyber Security Services
KPMG in the US

Key elements of the zero trust approach

The four key elements of zero trust are the single sign on, multi factor authentication, context inspection and anomaly detection.



Continue on your zero trust journey — or start today

The oil and gas industry is a particularly inviting target for cybercriminals. It is a financially lucrative enterprise, it plays an outsized role in meeting the needs of billions of people around the world, its operations are widely dispersed, and its accumulated technology debt and outdated cyber defense systems have left it vulnerable. It's time to move forward and reimagine these defensive capabilities by utilizing a zero trust approach.

Zero trust is flexible enough to be adapted to meet the needs of your organization, its culture and its workforce. Most oil and gas companies already have some manner of zero trust enabled technologies within their network environments. So for them, it's a matter of building on what they have already towards a stronger, more complete zero trust world. Whether you have parts of a zero trust program in place or are starting from scratch, keep in mind that it can be matured over time depending on your resources and readiness level. But the key is to get started or continue on your journey.

How KPMG can help

KPMG firms can help organizations implement zero trust models starting with strategic business case orientation, helping create roadmaps leading all the way up to technology integrations and implementations. Our professionals understand oil and gas systems, processes, and complete cyber challenges. Our first-hand experience with industry operations and cultures can help determine the best method and technology options to solve the most complex and urgent cyber security challenges while strengthening your organization's ability to handle emerging and evolving threats.

Cyber security regulation, malicious actors, acts of nature, and accidents will not slow down while organizations leaders are thinking about their next cyber security steps. Start planning or continuing your zero trust model implementation now so your organization is more prepared for what might happen next.

Zero trust as the future security design
Provide a strategic path and architecture solution design based on zero trust principles. Demonstrate current-state maturity, develop zero trust design, and deliver roadmap for integrated future solutions.

Accelerate zero trust adoption
Implement key solutions that are building blocks of zero trust journey — e.g., Build the Target Operating Model, Advanced/ Risk-based access model, network segmentation/SDP, proxy architecture, and API security and management.

COVID-19 and SolarWinds
Embed zero trust models and solutions as part of organization's digital transformation, supply chain, and shift-left security initiatives.

Alliances and technology leadership
Support program and technology transformation by leveraging our ecosystem of alliances and partnerships with leading zero trust products and technology solutions.

About the authors

Ronald Heil
Partner, Global Cyber Security Leader
for Energy and Natural Resources
KPMG in the Netherlands
E: heil.ronald@kpmg.nl

Ronald is a partner at KPMG in The Netherlands and is the Global Cyber Lead for the Energy and Natural Resources sector. He has extensive experience helping international companies in the banking, insurance, health, entertainment and other industries connect their products and devices to the Internet of Things and providing complex IT security and ICS/SCADA advice.

He specializes in large scale penetration testing services in industrial and other environments, including complex technical challenges and computer security incident response services, networking & infrastructure security design and review (e.g., complex Cloud services) and large scale IT Audit services.

Manuel Kanagasuntherie
Senior Manager, Cyber Security Services
KPMG in the UK
E: manuel.kanagasuntherie@kpmg.co.uk

Manuel is an experienced Enterprise Architect focused on Cybersecurity with a 20-year track record for delivering successful results across a wide range of programs including Digital Transformation (Cloud), Architecture transformation (Enterprise, Security and Zero Trust), M&A and Divestitures, Vendor Management, and Target Operating Model for global client base. He has architected and led digital transformations, developed cyber strategies, developed and implemented new operating models and as well as significant technology enabled business change & culture programs.

Dani Michaux
Partner, EMA Cyber Security leader
KPMG in Ireland
E: dani.michaux@kpmg.ie

Dani is the leader of the Cyber Security EMA practice and is the Head of the Cyber Security practice in Ireland. She previously led the Cyber Security and Emerging Technology Risk Practices for KPMG in Malaysia and the ASPAC region and KPMG's global IoT working group. Dani has worked with government agencies on national cyber security strategies and with international regulatory bodies on cyber risk agenda and regulatory landscape. She also is an advocate for inclusion & diversity, and women participation in computer science and cyber degrees.

Brad Raiford
Director, Cyber Security Services
KPMG in the US
E: braiford@kpmg.com

Brad Raiford is national lead for IoT & OT Cyber Defense for KPMG in the US. Brad focuses on embedding the principles of cyber-informed engineering into IoT/OT zero trust transformation, trusted autonomy, and cyber automation architecture. He has vast experience working with US and international companies building solutions for challenges today and beyond tomorrow.

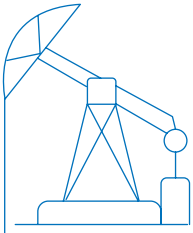
KPMG's Global Energy Institute

The KPMG Global Energy Institute (GEI), launched online in 2007, is a worldwide knowledge-sharing platform detailing insight into current issues and emerging trends within the gas, oil, power, and utilities industries. The GEI helps to shed light on key topics ranging from upstream volatility, midstream constraints, and industry consolidation, shifting customer demands and new technologies, alternative and renewable energy, smart grid technology and transformation, evolving regulatory and statutory requirements, as well as financial reporting and tax updates.

The GEI interacts with its over 40,000 members through a variety of channels, including webcasts, publications and white papers, podcasts, events, and quarterly newsletters. The institute works together with member firm clients, external partners and the global KPMG network of energy experts in analyzing the some of the most pressing challenges facing the industry and in developing practical solutions for an increasingly complex energy environment.

A complimentary GEI membership is an effective way for energy executives to gather the latest information on trends affecting the industry and help meet their continuing education requirements. Members receive early alerts and invitations to thought leadership, studies, events, and webcasts about key industry topics.

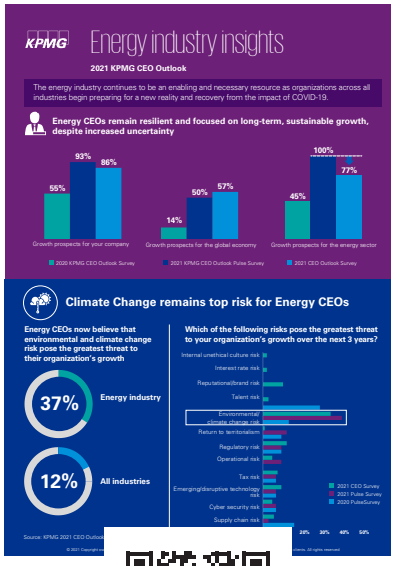
To receive timely updates and insights relevant to the oil and gas industry, become a member of the KPMG Global Energy Institute today by visiting home.kpmg/energy.

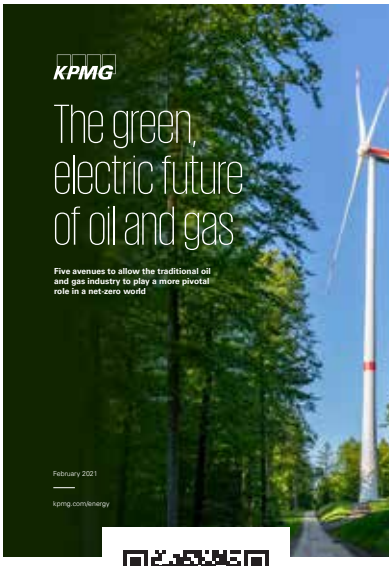


The GEI interacts with its over

40,000

members through a variety of channels, including webcasts, publications and white papers, podcasts, events, and quarterly newsletters.





KPMG Cyber Security Services

KPMG professionals have a deep industry-specific understanding of information security challenges in the Energy and Natural Resources (ENR) sector, including IT and OT within power and utilities, oil and gas, renewables, chemicals and mining. KPMG's global Cyber Security Services is an award-winning market leader in Cyber Security Consulting. Our cyber security capabilities are truly global, with over 3,200 information security professionals across the world

KPMG Cyber Security Services offers a four-pillar approach to present a globally consistent set of services. These services are aligned to clients' business priorities to provide reassurance and help them address the challenges that they are tackling.

Strategy & governance

Turn risk into competitive advantage.

Helping clients determine the appropriate levels of acceptable risk and understand how best to align their cyber agenda with their dynamic business and compliance priorities

Transformation

Accelerate your initiatives in an agile world.

Helping clients build and improve their programs and processes, supported by the right organization and technology, to improve their cyber agenda

Cyber defense

Confidently seize opportunities.

Helping clients maintain their cyber agenda as their business and technology programs evolve by providing greater visibility and understanding of changing risks

Cyber response

Operate with confidence in a digital world.

Helping clients effectively and efficiently respond to cyber incidents and conduct forensic analysis and detailed investigations. A holistic, adaptive strategy aligned to your business goals

Aligned with client business priorities and compliance needs

Services across all pillars:

- Operational technology security, resilience and transformation
- Digital cyber security — Cloud | Mobile | Internet of Things | Intelligent Automation | Blockchain
- Secure automation

Annually, KPMG is identified as a leader across many key analyst reports that affect clients' most pressing business challenges.

KPMG brand recognition among Energy and Resources consulting firms.

KPMG rated as most familiar brand for Energy and Resources consulting from a list of the world's top 15 consulting organization. KPMG also earned top marks for quality by Energy and Resources clients. This recognition includes ranking second for quality of work in data and analytics and third for quality of work in risk management (including cyber security) by clients in the Energy and Resources sector.

Based on 238 responses to a survey of senior clients of consulting firms and featured in *Perceptions of Consulting in Energy & Resources in 2021* published by Source Global Research.

KPMG brand and risk consulting services received top score by clients and prospects.

KPMG ranked number one for 'current brand score' among risk advisory firms and for the quality of our Security services. KPMG received the highest score of the 16 vendors evaluated in this category — a high achievement determined by clients and prospects alone. This ranking is based on mindshare, our level of credibility, authority, and competitive resilience — and topping this ranking recognizes our brand as the strongest in clients' minds today.

Based on 300 responses to a survey of senior clients of consulting firms and featured in *Perceptions of Risk Firms in 2021* published by Source Global Search.

For more information about Source and it's research please visit: www.sourceglobalresearch.com

Acknowledgments

This magazine would not be possible without the collaboration from colleagues around the world who generously contributed their support, knowledge and insights into the planning, analysis, writing and production of this report. Thank you to Tzouliano Chotza, Lyndie Dragomir, Nicole Duke, Mark Hamilton, Carmen Millet and Richard Turitz.

Contacts

Regina Mayor
Global Head of Energy
KPMG International
E: rmayor@kpmg.com

Valerie Besson
Regional Energy & Natural Resources Leader for Europe/Middle East/Africa (EMA) and National Sector Leader, Energy and Utilities
KPMG in France
E: valeriebesson@kpmg.fr

Manuel Fernandes
Regional Energy & Natural Resources Co-Leader for Americas and National Oil & Gas Leader
KPMG in Brazil
E: mfernandes@kpmg.com.br

Ronald Heil
Global Cyber Security Leader for Energy and Natural Resources
KPMG in the Netherlands
E: heil.ronald@kpmg.nl

Angela Gildea
Regional Energy & Natural Resources Co-Leader for Americas and National Sector Leader, Energy, Natural Resources and Chemicals
KPMG in the US
E: angelagildea@kpmg.com

Jonathon Peacock
Regional Energy & Natural Resources Leader for Asia Pacific (ASPAC) and Oil & Gas Leader
KPMG Australia
E: jjpeacock@kpmg.com.au

home.kpmg/drillingdown

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name:Drillng Down
Publication number: 138002-G
Publication date: April 2022