Plugged In

Power and Utilities Magazine

First edition

Articles include:

From globalism to national security

ESG and cyber security are two sides of the same coin

Incident readiness: a playbook for your worst day

From continuity to resilience

KPMG in Belgium

Contents

01

Foreword

Decarbonization and electrification are twin trends that have come to define modern energy systems. The power and utilities (P&U) sector, particularly electricity generation, is undergoing dramatic change as a consequence. Renewable energy, both grid-scale and distributed, coupled with the digital revolution, alters the grid's topology and adds colossal complexity to the electricity supply chain.

Digital connectivity has also exposed networks to cyberattacks from malicious nation-state hackers and criminal gangs. Amongst a growing list of incidents are a suspected state-sponsored assault on India's power grid via IoT devices and cameras[1] and an attempted poisoning of Florida's water treatment system.[2]

Climate-related weather events like fires, flooding, winds and extreme heat and cold are a further threat, accentuating the vulnerabilities of aging assets and raising the specter of lawsuits for damage to the environment and people.

All this comes as the sector faces a surge in demand as the world recovers from the COVID-19 disruption, along with high energy and commodity prices exacerbated by the war in Ukraine. Customer expectations are changing rapidly, with consumers seeking new, digital engagement channels while also becoming suppliers to the grid through self-generation.

It's no exaggeration to say that electricity underpins nearly every facet of modern life — without which our daily existence is threatened. To deliver the 24/7 service that society demands, P&U providers must remain solvent, efficient and secure in a volatile market with high capital and maintenance costs and talent scarcities. Additionally, regulators are placing higher demands on the P&U sector to demonstrate it has done everything it can to avoid outages.

In this first edition of *Plugged In* magazine, we look at how companies can face up to the increasing levels of risk in the P&U sector to remain resilient and continue to power people, organizations and nations.

From globalism to national security discusses how the conflict in Ukraine has altered notions of global energy supply chains while looking at ways to tackle this and other risks like cyber, distribution, investment and asset management.

Anish De
Global Sector Lead,
Power & Utilities,
KPMG National Leader,
Energy, Natural Resources
& Chemicals,
KPMG in India

[1] Business Standard, Suspected Chinese hackers collect intelligence from India's power grid, April 2022

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

In ***ESG and cyber security are two sides of the same coin***, we argue how trust in renewable power sources can drive the decarbonization revolution — by overcoming the threats caused by cyberattacks on a distributed grid.

Another article, ***From continuity to resilience***, charts the shift in focus from 'response and recovery' to 'resilience by design' to maintain services 24/7 through strategies like infrastructure hardening, weather event modeling, improved cyber security, and access to the right skills.

The fourth and final piece, ***Incident readiness: a playbook for your worst day***, takes a realistic view of the various threats and considers how P&U providers can keep on top of risks, to prevent them in the first place and be fully ready should the worst happen, to minimize the fallout.

Technology will play an increasing role in risk and resilience, with automation, AI, IoT and VR/AR helping to simulate the impact of future attacks and weather events, increase control and monitoring over networks, identify breaches, adapt swiftly and trigger recovery. 5G will likely be at the center of these efforts, while the emerging metaverse can open up new opportunities to test, communicate and learn new capabilities.

It's an exciting yet challenging time for the P&U sector, and KPMG professionals are working with clients at the cutting edge to help power the future.

Enjoy the articles!

02

From globalism to national security

Evolving risks in the power and utility sector

By: Valérie Besson, Anish De, Robert Johnston, and Stefano Moritsch

The war in Ukraine has dramatically altered perceptions of energy security and accelerated many countries' decarbonization agenda.

Since the tanks rolled across the Ukrainian border, many power & utilities (P&U) providers had to rethink their energy supply strategies. Having become accustomed to a global market dictated primarily by price, the sector is now adjusting to the idea of sourcing energy only from countries considered political allies.

The European Union (EU) has pledged to cut its gas supply from Russia by two-thirds by the end of 2022, agreed on a partial ban on Russian oil[1] and announced a deal to buy an additional 15 billion cubic liters of LNG (liquified natural gas) from the US to reduce its dependence on Russian energy.[2] In a way, geopolitical imperatives are now pushing the EU to dramatically accelerate its net zero ambition, as exemplified by its RePower EU plan.[3] Even regions less reliant on Russian imports to power their economies will still feel the effect of global energy price volatility in the wake of supply dislocation, western sanctions, as well as self-sanctioning by companies who are wary of reputational damage, a stark reminder of the importance of stable, resilient energy supply chains.

In addition to seeking new conventional energy suppliers, governments, especially in Europe, will be pushing for greater energy efficiency, accelerating the transition to renewables, and investing in nuclear power.

The P&U sector was already undergoing huge disruption before the war, with society's shift to all things electric, the green energy revolution reshaping grids, and digitalization shaking up ways of working. Add to this evolving geopolitical, supply chain, environmental, investment, cyber, talent, and cost risks, and companies must cope with an uncertain future.

> "Having become accustomed to a global market dictated primarily by price, the sector is now adjusting to the idea of sourcing energy only from countries considered political allies."

[1] Bruegel, Europe's Russian oil embargo: significant but not yet, June 2022

[2] BBC, EU signs US gas deal to curb reliance on Russia, March 2022

[3] European Comission, REPowerEU: A plan to rapidly reduce dependence on Russian fossil fuels and fast forward the green transition, May 2022

Geopolitical/supply chain risk: rewriting the global energy map

One consequence of the decoupling from Russian energy could be the division of the world into new energy blocs of countries broadly sympathetic to each other — such as the Atlantic (the US and Europe), China, India and Russia, with the Gulf and other non-aligned countries possibly supplying both blocs (unless secondary sanctions become an option).

Such a move would radically change global supply chains as P&U providers look for immediate alternative sources, including LNG from the US and other regions, to satisfy domestic demand from consumers and energy-intensive industries like steel, manufacturing and chemicals.

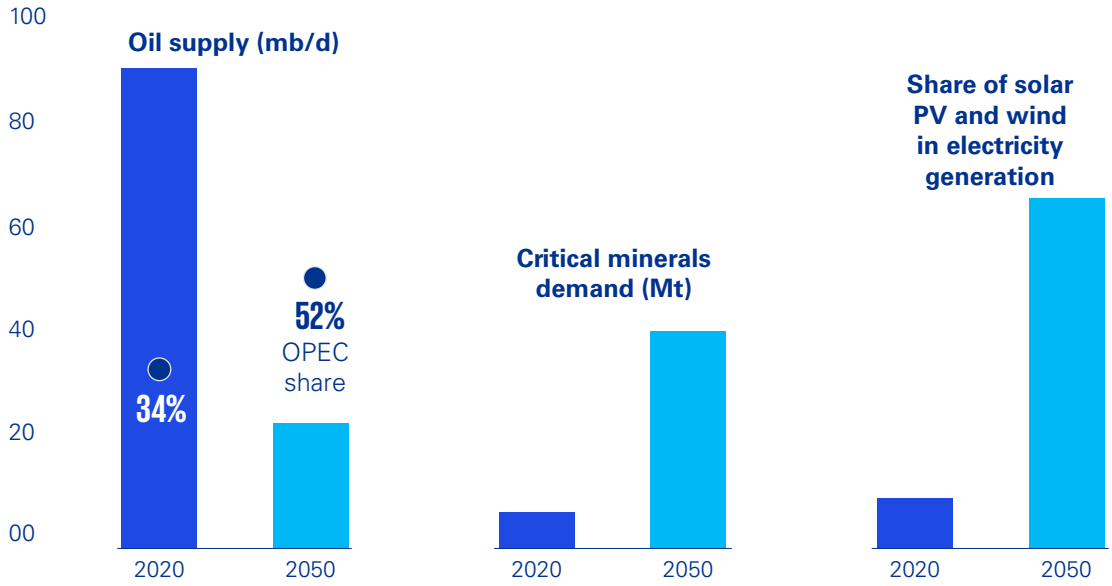
Supply chains for nuclear, hydrogen and renewable energy components, especially uranium, batteries, solar and wind power, will likely come under more significant pressure as the race for alternatives intensifies.

COVID-19 had already exposed vulnerabilities of globally interdependent supply chains as P&U players struggled to access critical resources throughout the pandemic. Now that Russia, Ukraine, and possibly other neighboring countries have effectively been cut out of supply chains, it's vital to find new, reliable sources swiftly.

Those countries at an earlier stage in their energy transition face difficult choices, as they have fewer alternatives to fossil fuels and won't want to risk blackouts or industrial disruption.

Action: Define the key risks to your organization's footprint, monitor events, and plan scenarios encompassing different election results, security developments, and national ideological trends. If feasible, explore the possibility of risk-proofing supply chains by duplicating them across like-minded regional/ideological blocs to limit exposure to geopolitical uncertainty.

Global energy security indicators in the net zero pathway



Note: mb/d = million barrels per day; Mt = million tonnes.

Source: IEA, Net Zero by 2050: A Roadmap for the Global Energy Sector, May 2021

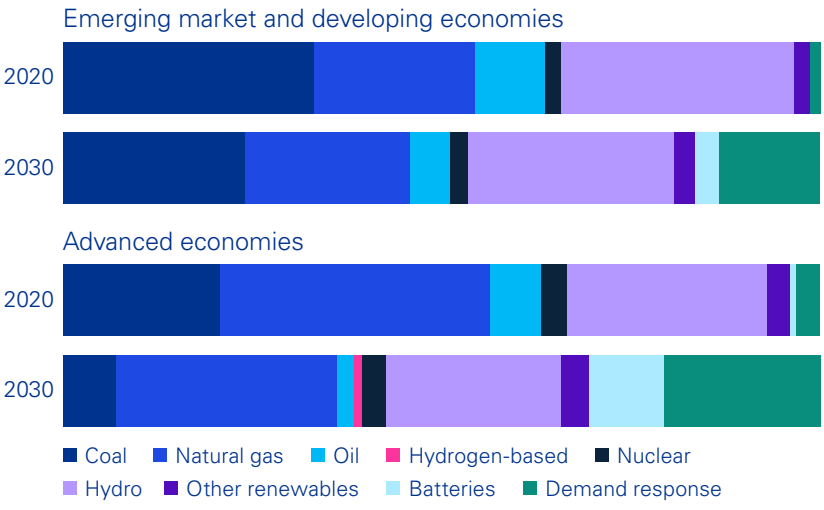
Investment risk: driving decarbonization

For some governments, especially in Europe, the shock of reducing dependence on Russian gas and, to a lesser extent, oil has made them even more determined to decarbonize their economies. The EU's 'Fit for 55' proposal (to cut greenhouse gas emissions by 55 percent by 2030) continues to be a significant driver of investment. China has committed to reducing its carbon footprint, with the subsequent associated costs in the short term.

The US also has ambitious clean energy plans. However, with its abundant shale gas and oil supplies, it will remain a fossil fuel player to meet domestic consumption and satisfy global demand. Australia has been relatively unaffected by events in Europe and has rich seams of coal, gas and other natural resources. But it also has a solid green agenda, with many solar and wind projects in progress. Almost one-third of Australia's electricity in 2021 came from renewable sources — a 5 percent increase on the previous year.[4]

Net zero targets place considerable pressure on governments and private P&U operators to invest in carbon-free technologies. It's a similar story with the anticipated renaissance of nuclear, which is expected to play a more prominent role in the energy mix. Establishing secure energy capabilities requires a wide range of capital-intensive infrastructure to achieve electrification of transport and other parts of the economy. These efforts are primarily on a country-by-country basis rather than collective, cross-border initiatives, with different nations traveling at varying speeds.

The huge investment required to achieve net zero may strain economies only starting to emerge from a pandemic-induced recession.



Electricity system flexibility by source 2020 and 2030[5]

Action: At an industry level, P&U providers should work towards their organizational decarbonization targets, cut emissions, and carry out robust ESG reporting to demonstrate that they're on track. Regulated businesses should align their goals with the latest regulations or alternatively seek approval when there is ambiguity, if regulations allow so (which is the case in certain jurisdictions). For companies operating in non-regulated segments or where direct regulatory cover is not available, the appropriate approach is to look for financing instruments that explicitly cater to their circumstances. Transition financing is receiving a lot of attention, with regulatory authorities and financiers explicitly addressing transition needs and taking on board associated risks. In this way, they can gain a degree of cover for their investment risks.

[4] Clean Energy Council, Clean Energy Australia Report, April 2022

[5] IEA, Electricity system flexibility by source in the Net Zero Scenario, 2020 and 2030, October 2021

Cyber risk: growing threats across a vast attack surface

P&U assets are increasingly recognized as vital to national security. Given the sanctions and other actions taken against Russia, and the support for Ukraine, the threat of retaliation is exceptionally high in the form of hacking, ransomware, and malware. This is on top of other nation-state actors, cybercriminals and hacktivists. The geographical scale and complexity of P&U organizations mean that attack surfaces are broad, with the risk of putting power plants, generators and wind turbines out of action; remotely disconnecting grids to halt transmission and distribution to customers; and attacks on IoT, devices and electric vehicles, leading to the theft of customer information, billing fraud and disrupted services.

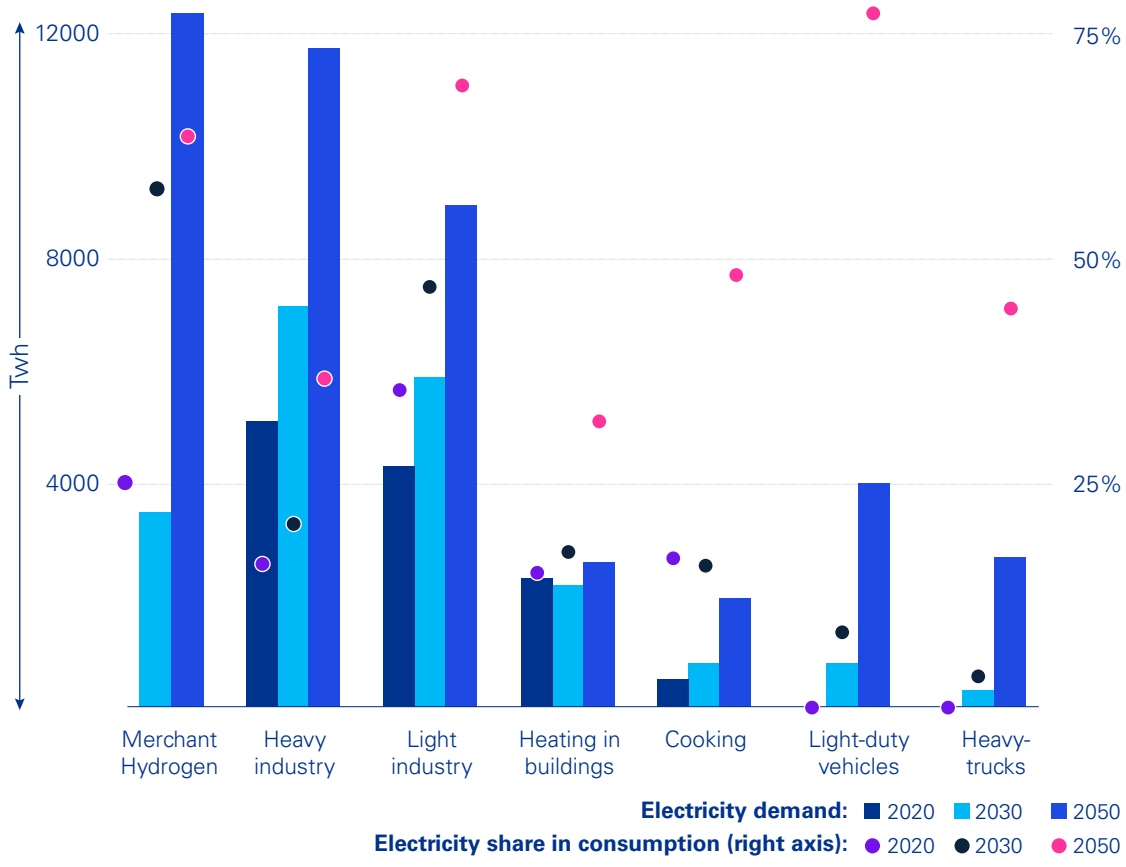
Action: To be fully prepared, P&U providers should review their business continuity plans, assess the vulnerabilities along the supply chain, and conduct exercises for recovering after a breach. Building a cyber-aware culture will help avoid the prospect of an attack and improve incident reporting. And with growing regulatory expectations, formal monitoring and reporting have become a high priority. Given the potential for nation-state attacks, the P&U industry as a whole must work with the government to tighten defenses and improve the capability to respond.

Distribution risk: meeting evolving customer demands

The topology of power generation is changing with a transition to a more distributed, decentralized grid, with many new players — often able to generate their own (renewable) electricity and sell it to others. All of which shifts power to consumers and threatens P&U revenue streams, as customers find it easier to switch suppliers or even produce power themselves — aided by rapid digitization. Network management grows in complexity, and P&U companies must ensure they balance energy supplies from the many providers to avoid suffering reputational damage.

Action: It's vital to build resilience into the grid through more effective scenario planning to predict demand and plan accordingly to avoid outages. P&U companies should work closely with other grid stakeholders and build redundancy into the system so that one failure doesn't bring down the whole network.

Global electricity demand and share of electricity in energy consumption[6]



Notes: Merchant hydrogen = hydrogen produced by one company to sell to others. Light-duty vehicles = passenger cars and vans. Heavy trucks = medium-freight trucks and heavy-freight trucks.

[6] IEA, Net Zero by 2050: A Roadmap for the Global Energy Sector, May 2021

Climate change risk: maintaining assets

Wildfires, in particular, pose a substantial risk to P&U providers. With thousands of kilometers of gas pipelines and electric power lines, a minor fault in equipment can quickly spark off a new fire. Companies can suffer hefty fines — and convictions for manslaughter — if they're found to have involuntarily started wildfires by failing to maintain infrastructure adequately.

Climate change has brutally exposed aging infrastructure and puts pressure to preserve and replace assets and trim back surrounding vegetation. Assets are also highly vulnerable to other impacts of climate change, such as floods, winds and freezing weather, increasing in frequency and intensity.

The increasing occurrence of severe weather events places a growing insurance risk, pushing up premiums to a point where they impact margins. All the more reason to improve defenses.

Action: Tools to help achieve greater resilience include risk models to detect the most at-risk infrastructure, visual and aerial inspections, vegetation management, monitoring cameras, satellite technology, and separating the grid into smaller sections to minimize damage. Proactive power shut-offs are the last resort, turning off electricity when winds and dry conditions increase fire risk. And, of course, P&U companies should invest in assets to help ensure they're robust enough to cope with modern-day pressures.

Talent risk: appealing to a new generation of workers

Like many sectors, P&U organizations face competition for people, exacerbated in some parts of the world by the great resignation accompanying the pandemic. Turnover in P&U was already relatively high compared to other industries, made more urgent by an aging workforce approaching retirement.

Younger employees are more likely to want fulfilling experiences that give them opportunities to grow. Roles and careers need to evolve to meet these expectations, including increased use of technology and less top-down management. And providers will likely be under increasing pressure to show that they are building diverse workplaces.

Many of today's younger workers are driven by a new-age purpose to improve society and the environment. P&U organizations whose values and strategies align with these principles are likely to be more attractive to this new generation. In addition, fewer plan long careers in one organization, so a higher churn may become the norm and something that companies must plan for. It will be important to build a critical mass of capabilities in core functions that are managed internally to cope with higher employee turnover. For non-core or thinly staffed operations, or in areas where it's hard to recruit and retain specific, in-demand skills, the use of outsourced/gig economy workers may be necessary, especially from agencies with a bench strength of specialized talent.

> "Roles and careers need to evolve to meet these expectations, including increased use of technology and less top-down management."

Action: Attempts should be made to improve the industry's attractiveness to new candidates and retain existing workers, moving away from hierarchical structures and encouraging innovation. Hybrid working can help with these efforts, to create the kind of flexibility that workers of all generations are looking for. As the digital revolution gathers pace, cultural and organizational change will be necessary to create an environment that encourages innovation in decarbonization and distribution.

Cost risk: Coping with volatility

Oil and gas prices, already high since the COVID-19 recovery, have soared since the conflict in Ukraine began. Governments may come under pressure to subsidize energy, fearing that inflation could provoke civil unrest. The cost of power generation has risen in line with commodity, oil, and gas costs.

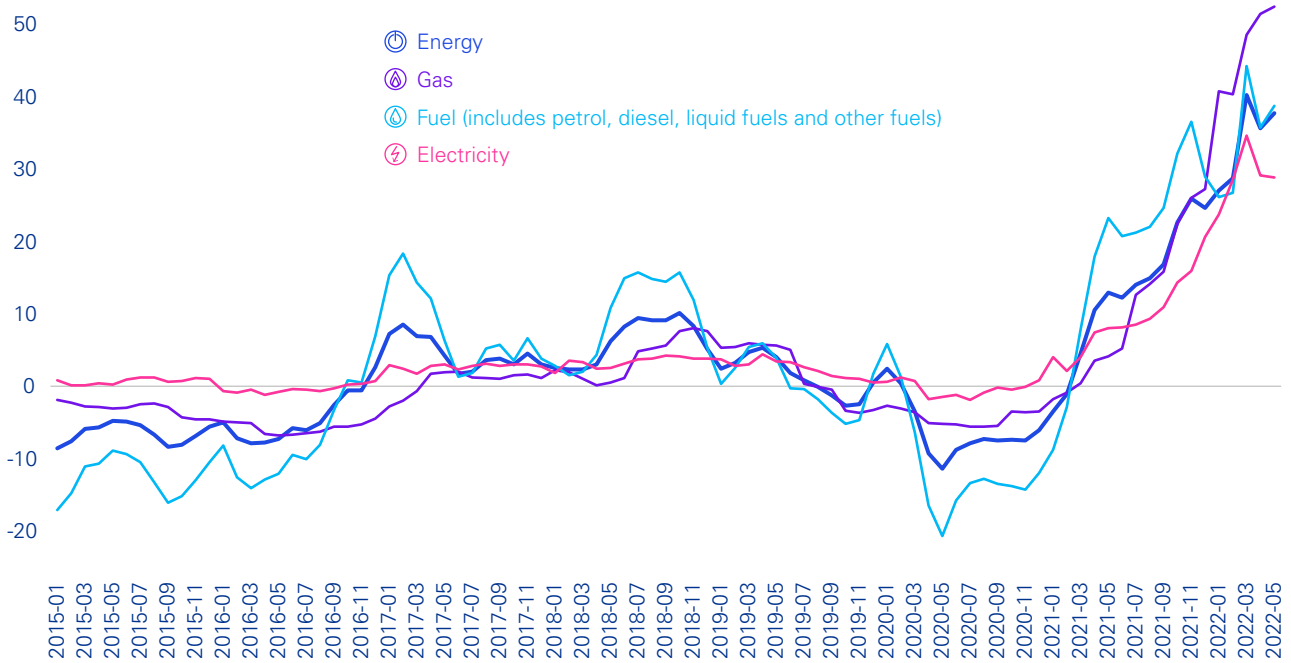
Some of these increases can be passed onto businesses and consumers in a regulated sector, but there is often a cap, which inevitably hits profitability. Coping with such volatility is challenging, and sourcing alternatives like LNG or shifting to renewables cannot happen overnight.

P&U providers will be assessing how they can improve operational efficiency and productivity to avoid having to pass on too much of the higher input costs to customers.

Action: Governments, regulators and providers can foster more significant energy efficiency, working with investors, regulators, power companies, and the wider business community to help incubate new startups and change consumer and business habits.

European Union energy prices in the last 5 years[7]

(annual rate of change)



[7] Eurostat, Harmonised index of consumer prices (HICP) — monthly data (annual rate of change), May 2022

Towards a resilient future

Energy transformation and energy security are increasingly seen as complementary goals. As P&U providers plan a resilient future, they must gain more reliability over the supply of traditional fossil fuels while securing the investment in renewables — and possibly nuclear — to achieve a level of diversity that will make them more self-sufficient.

The war in Ukraine has demonstrated how quickly situations can change. Add cyber threats and climate-related risks into the mix, and there's even more reason to establish strong resilience and incident response planning to keep vital national assets operating in a volatile world.

Much of what may happen is out of the control of the P&U industry. However, here are some steps to help your organization be as well-positioned and prepared as possible regardless of what occurs in 2022 and beyond:

1. Prepare a plan to manage activist investors and other stakeholders, who increasingly use ESG (environmental, social and governance) issues to open the door.

2. Review your organization's 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 government involvement.

4. Understand how proposed legislation and government actions could affect your company: does your organization have 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. 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.

7. Review your organization's cyber defense protection: the risk of a cyber breach is perhaps the most underestimated above-ground risk in the P&U sector. It cuts across political and geographical risks, and any company, regardless of size, is a potential target. You are vulnerable to a cyber security breach no matter where you operate.

About the authors

Valérie 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

Valerie has 20 years of experience in audit including 6 years overseas, respectively, in the KPMG member firm offices of Bucharest, New York and Short Hills.She has worked in various lines of business, including Industrial Products, Consumer Markets, Energy, Chemicals and Pharmaceuticals, and Information, Communication and Entertainment. She has been involved in many engagements besides audits, such as financial due diligence, IFRS and US GAAP conversions, carve-out audits, participation in IPOs, etc. Currently, Valerie specializes in French-listed clients.

Anish De
Global Sector Lead, Power & Utilities, KPMG National Leader, Energy, Natural Resources & Chemicals
KPMG in India
E: anishde@kpmg.com

Anish is KPMG's Global Head for Power & Utilities and National Head for Energy, Natural Resources and Chemicals for KPMG in India. He has over 25 years of experience in energy sector consulting. As a renowned power sector expert, Anish has undertaken pioneering work in sector reform and restructuring, designing sectoral policy and regulatory frameworks; commercial and financial advisory; PPP; strategic planning, economic analysis; investment frameworks; corporate strategies, turnaround plans, institutional strengthening, and capacity building; power markets; energy efficiency; smart grids and digital.

Robert Johnston
Special Advisor for Energy and Climate
Eurasia Group
E: johnston@eurasiagroup.net

Robert ("RJ") is Special Advisor on Energy and Climate to Eurasia Group. RJ founded the firm's Energy, Climate, and Resources practice in 2006 and served as the firm's CEO from 2013 to 2018, overseeing a period of rapid growth and international expansion. RJ has 25 years of experience working closely with corporate and institutional investor clients in the oil and gas, mining, electric power, and cleantech sectors on strategy, risk assessment, government relations, and communications around policy, markets, and geopolitics.

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 joining the dots between the macro-political trends and their commercial implications in various sectors, Stefano helps global businesses not only survive but thrive in geopolitical volatility. He helps identify the 'so what' of macro trends through strategic scenario planning, due diligence and geopolitical risk management. With an academic background in international relations, diplomacy and international law, Stefano is eager to bring to the role several years of management consulting practice in Australia, assisting corporate clients, industry associations, and government clients to navigate complex regulatory environments worldwide.

03

ESG and cyber security are two sides of the same coin

In the transition to green energy, the key currency is trust.

By: Prasanna Govindankutty, Ronald Heil, and Kristy Hornland

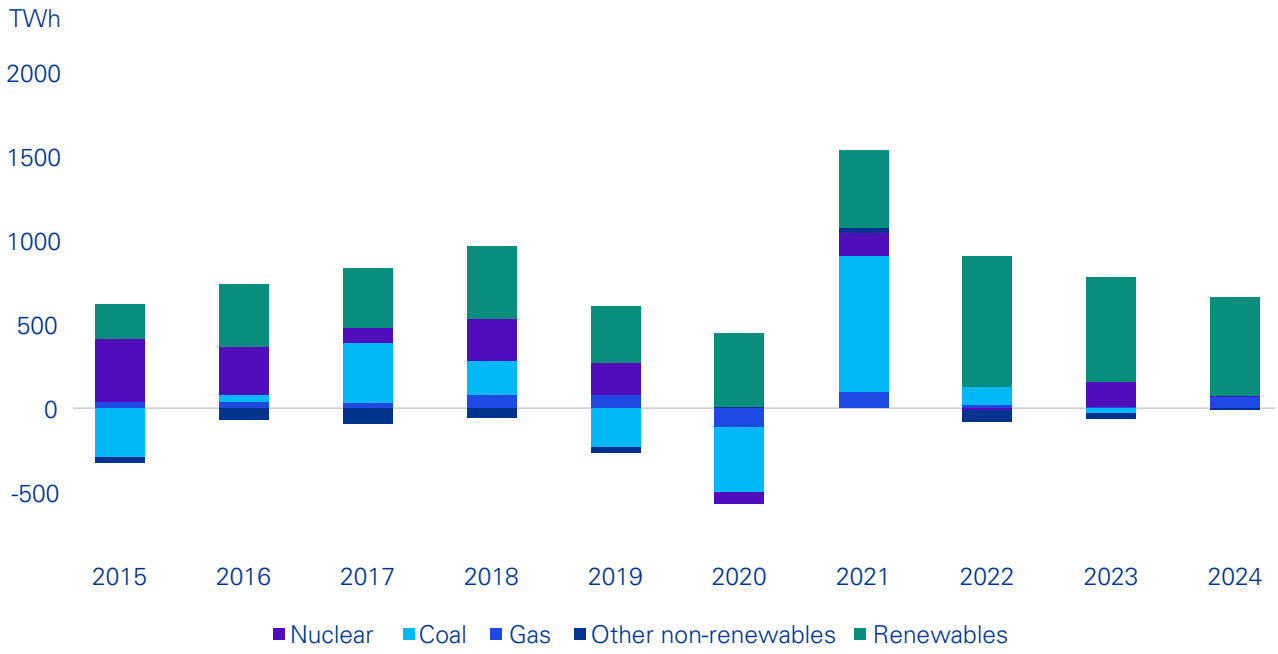
Amid a brutal war in Eastern Europe, there's a lot of focus on energy security. Countries with a higher proportion of renewable sources may feel better placed to withstand volatile fuel supply chains and continue to power industry, commerce and public services.

Many countries have pledged to accelerate their transition to renewable energy. Germany — which is highly dependent on Russian gas — has announced plans to give up coal entirely by 2030, 8 years ahead of its original target. It now aims to get 80 percent of its electricity from renewable sources by 2030. France and Austria are going in a similar direction, while Poland, one of Europe's heaviest coal consumers, is making significant investments in wind power.[1]

Such ambitions align with the UN Strategic Development Goals and resonate with citizens, governments and investors. But, with the world becoming ever more dependent upon electricity, renewables must pass the trust test and demonstrate that they can offer the 24/7 reliability that users expect. Failure to do so could severely undermine the decarbonization revolution.

"Such ambitions align with the UN Strategic Development Goals and resonate with citizens, governments and investors."

Global changes in electricity generation[2]



[1] National Geographic, How the Ukraine war is accelerating Germany's renewable energy transition, May 2022

[2] IEA, Global changes in electricity generation, 2015–2024, Jan 2022

Complexity brings additional cyber threats

Renewables bring greater energy independence, as the power is generated closer to those who need it, from sources within national boundaries. Microgrids take this concept one step further, enabling smaller providers and individual consumers to produce, store and distribute clean power. One US study suggests that a decentralized grid could alleviate stress on the main power generators and meet 20 percent of peak load by 2030.[3] This includes solar-powered batteries, delivering a highly reliable backup for business and government facilities.

However, distributed grids are also more complex and interconnected, with thousands and possibly millions of new energy providers, including private homes, fitted with smart meters connected to personal mobile devices. Add to this the increasing digitization of power station operational technology (OT), including numerous IoT to track performance and carbon capture. The result is a broader range of attack points. In increasingly interconnected systems, nation-states and criminals have multiple opportunities to hack into the primary grid via individuals or organizations who may have weaker cyber security.

Traditional OT systems are sometimes too old to receive security updates yet are linked to other internet-facing areas of the network and the broader software supply chain. A further threat comes from connected battery management systems that monitor safety and reliability. And software-defined electricity, which increases the efficiency of electricity generated by any renewable source, also contains code vulnerable to hackers.

In a recent survey by risk manager DV, less than half (47 percent) of energy professionals believe their OT security is as robust as their IT security. Six out of 10 say their organization is now more vulnerable than ever to an attack.[4]

Then there are home car chargers and, ultimately, ubiquitous connectivity for electric vehicles, which could bring transport to a standstill and cause accidents. And our increasing reliance on renewable electricity can strain grids, especially if storage batteries go down for any reason. An outage can take out drinking water systems, wastewater facilities and the communications infrastructure — impacting every aspect of daily life. Furthermore, battery storage can be considered a greater fire risk.

There have been several alleged cyberattacks on European wind-energy companies — either directly or through their suppliers — since the Russian invasion of Ukraine.

In one incident, German company Enercon suffered disruption to more than 5000 wind turbines following an attack on its satellite broadband provider Viasat. A notorious ransomware gang reportedly claimed responsibility for at least one hack and says it will share internal chats and source code with Russia.[5]

These various and rising threats could hold back the adoption of renewable energy by governments and P&U companies. If consumers feel that green power providers could suffer more outages, they will be less likely to use their services. Enthusiasm for decarbonization may wane if people can't use their electric cars, wash their clothes or cook the evening meal.

One US study suggests that a decentralized grid could alleviate stress on the main power generators and meet 20% of peak load by 2030.

[3] The Brattle Group, Cost-Effective Load Flexibility Can Reduce Costs by More Than $15 Billion Annually, June 2019

[4] reNEWS, Energy industry must act 'swiftly' against cyberattack, May 2022

[5] PC Magazine, Hackers Reportedly Target Wind-Energy Companies, April 2022

Building and maintaining trust in decarbonization

Robust cyber security and reporting assure stakeholders that P&U companies have secure, resilient operations that prevent and recover from cyber and physical attacks and climate threats like wildfires, floods, winds, and extreme hot and cold temperatures.

Given the increasing cyber risk from Russia and other nation-states and criminal groups, robust cyber security culture and protocol can improve defenses and responsiveness. The priority is to protect critical assets that determine whether customers receive power, water or other vital utilities.

Strict data security rules and processes can make employees cyber aware and avoid breaches. Renewable assets are increasingly classed as critical infrastructure, which obliges operators to comply with the rising volume of cybersecurity regulations. Regulatory fines can provide a nasty wake-up call — and damage trust — but a cyber-aware organization should not act primarily on fear but on a desire to do the right thing and maintain customer service.

All P&U companies need a standard framework for measuring cyber risk, and transparent procedures for restoring service following an attack. Across the grid network, IoT sensors and other data gathering tools can help detect potential problems arising from cyber and physical aggression (as well as storms, fires and other natural phenomena).

There is a lack of global consistency for cyber security standards and practices and an urgent need to converge and share information to make the entire renewables industry more resilient, which can help ensure trust and hopefully speed up adoption. Given the unique role of P&U infrastructure in a nation's existence and the interconnected nature of energy, governments are likely to get more involved and collaborate with private players across the supply chain.

As P&U providers become ever more digital, their ESG and cyber strategies should align with data at the center. Data drives every ESG decision, whether evaluating suppliers' sustainability, tracking carbon footprint, measuring workforce diversity, spotting data leaks, and, most importantly, reporting ESG progress to meet growing demands for transparency.

Directors should stay abreast of evolving industry reporting standards and ensure that their organizations provide the required information and insights. Presenting robust corporate cyber, compliance, and risk policies are vital to winning the trust and managing the transition to ESG. Equally, the perceived poor performance of renewable assets can damage confidence in ESG and hold back governments' sustainable agendas.

ESG can bring benefits to the P&U sector as well as significant risks. By committing fully to the ethos of purposeful, sustainable business and building strong governance, P&U companies can play an essential part in helping societies become greener, more secure, and more resilient.

> "Strict data security rules and processes can make employees cyber aware and avoid breaches. Renewable assets are increasingly classed as critical infrastructure, which obliges operators to comply with the rising volume of cyber security regulations."

Critical elements of a resilient renewable power system

Governance
Appoint a senior executive responsible for cyber security risk and agree on the appropriate frequency of cyber risk reporting.

Assets
Keep on top of all assets that may need cyber protection.

Vulnerabilities
Understand any vulnerabilities and update such knowledge as threats evolve.

Monitoring
Continually monitor systems and assets.

Security compliance
Keep abreast of evolving industry standards and regulations for practice and disclosure.

Culture
Ensure that all employees receive comprehensive cyber security training, with senior cyber security professionals participating in industry knowledge-sharing forums.

Reporting
Track and report on the effectiveness of cyber security defenses and the source, volume and severity of incidents.

How KPMG can help

Taking a practice approach to your cyber security reporting can promote digital trust in your organization. KPMG firms can help deliver a range of services and change to approaches to enable your organization to create a trusted digital word, including:

- Cyber maturity assessments (CMAs) to examine posture of their current threat and risk landscape as well as compliance with present industry regulations
- Target operating model (TOM) and Change management development for governing your cyber program
- Partner with leading IoT/OT discovery platforms to help you discover your operational assets and sustain your visibility
- Managed service support for monitoring operational technology IDS/IPS alerting
- Vulnerability management programs to ensure your systems remain operational and protected
- Cyber training and awareness programs crafted for OT environments and personnel
- Advanced data analytics to assess the ongoing posture of your security program

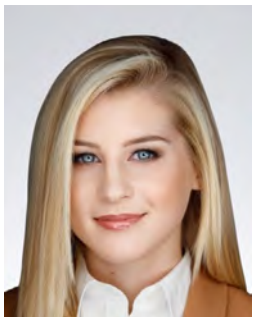
About the authors

Prasanna Govindankutty
Principal, Advisory,
Cyber Security Services
KPMG in the US
E: pkgovindankutty@kpmg.com

Prasanna leads Cyber Governance, Risk, and Compliance (GRC) services for KPMG in the US. In this role, he is responsible for the strategic direction of the service offering, including capability development, vendor partnerships and building teams. With two decades of consulting and industry experience, Prasanna helps clients comprehensively transform their cyber and technology risk management functions through tailored strategies and market-leading technologies.

Ronald Heil
Global Cyber Security Leader for
Energy & 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 & 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.



Kristy Hornland
Manager, Cyber Security Services
KPMG in the US
E: khornland@kpmg.com

Kristy is a manager within the US Cyber Security Defense practice and has spent the past 8 years working with utility clients to transform their security posture by designing, implementing, and operationalizing cyber data protection programs in mixed prem and cloud environments. She has deployed international and national utilities data protection programs (technologies and processes), allowing clients to improve their security posture and leverage cyber as a business enabler rather than a barrier. Kristy has developed thought leadership in the IoT/ OT space around emerging connected technologies and accompanying cyber risk and is a host of KPMG's Perspectives in IoT podcast.

04

From continuity to resilience

Our growing dependence on electricity makes it more critical than ever to build a proactive, resilient organization to ensure continuity of service.

By: Ali Abedi, Cassandra Hogan, Onur Karakus, and Ramsay Sawaya

“Too big to fail” is an over-used phrase, but it’s relevant and appropriate in the case of power and utilities (P&U).

Electricity underpins virtually every aspect of our lives. Yet, power generation and delivery are under a growing threat from natural disasters, cyberattacks, aging infrastructure and workforce, and supply chain interruptions. At the same time, the sector is getting to grips with complex, decentralized grid systems, renewable energy sources and digitization.

Power companies and utilities, public and private, have always been focused on keeping the lights on and the water running — but the changing nature of risks has shifted the emphasis from response and recovery to resilience by design to maintain services 24/7. Regulators expect higher operational, commercial, and financial resilience standards across the supply chain. The European Union’s proposed NIS 2 Directive could oblige P&U (and other industries) companies to demonstrate new levels of cybersecurity.[1] Failure to take adequate preventative measures can leave companies — and their leaders — open to fines and custodial sentences.

In this article, we take a deeper look at the main drivers of resilience and discuss how P&U companies can integrate these elements to maintain their services.

> “The European Union’s proposed NIS 2 Directive could oblige P&U companies to demonstrate new levels of cyber security.”

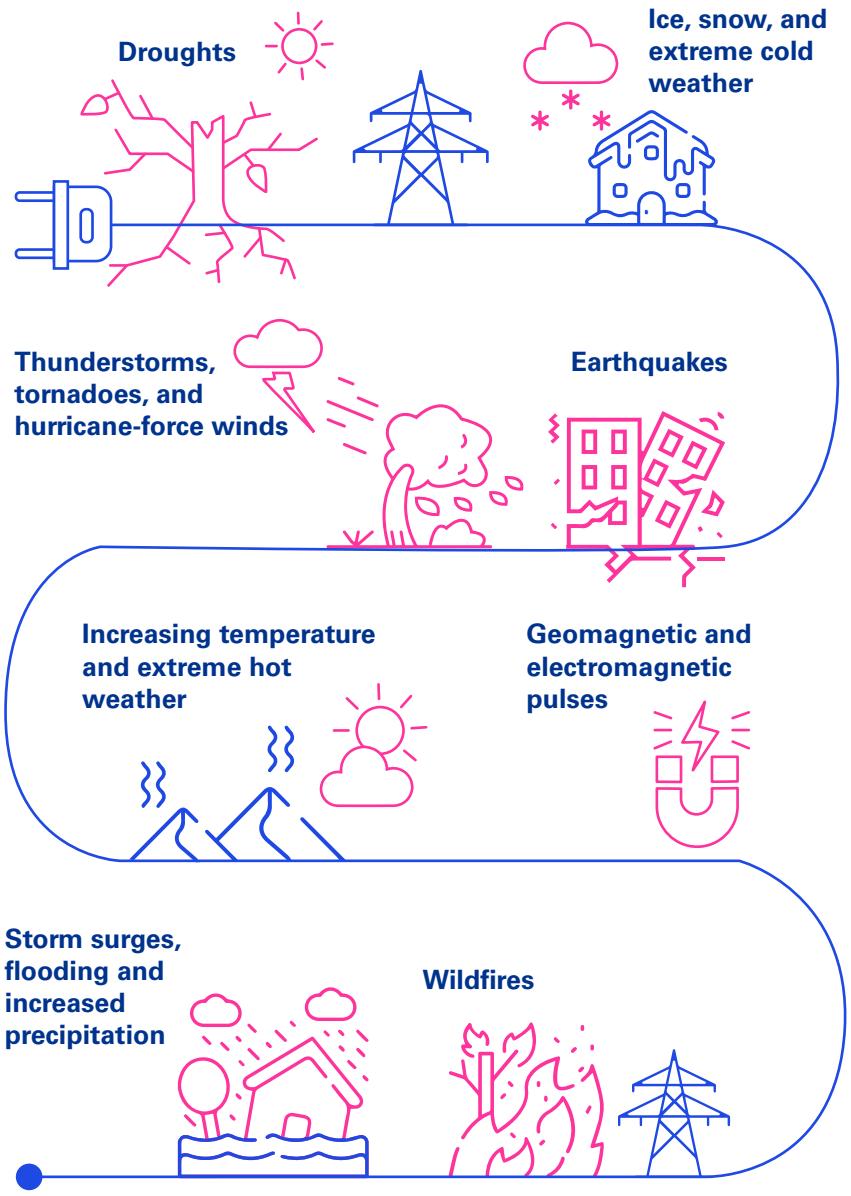
[1] European Commission, Commission welcomes political agreement on new rules on cybersecurity of network and information systems, May 2022

Natural threats

Climate change is a vast and growing concern for the sector. Storms, forest and bush fires, flooding, winds, extreme hot and cold, and droughts are no longer freak events but frequently occurring natural phenomena in many geographies. The US has suffered 323 weather and climate disasters since 1980, with estimated damage of US$2.195 trillion.[2] And between 2013 and 2020, the number of outage hours per year doubled from four to eight.[3]

In India in 2022, over a billion citizens have been struggling to cope with unbearable temperatures well over 40° Celsius — the hottest Spring in the country's recorded history, preventing outdoor working and causing power outages, water shortages, state-imposed rationing, train cancellations, as well as reducing industrial and agricultural output.[4]

In addition to damaging physical infrastructure, such phenomena can also hold up supply chains of vital parts and materials. And P&U companies don't just have to cope with the effects of climate change on their operations; they should also consider their own organization's impact on the environment and society, whether it's carbon emissions or treatment of workers.

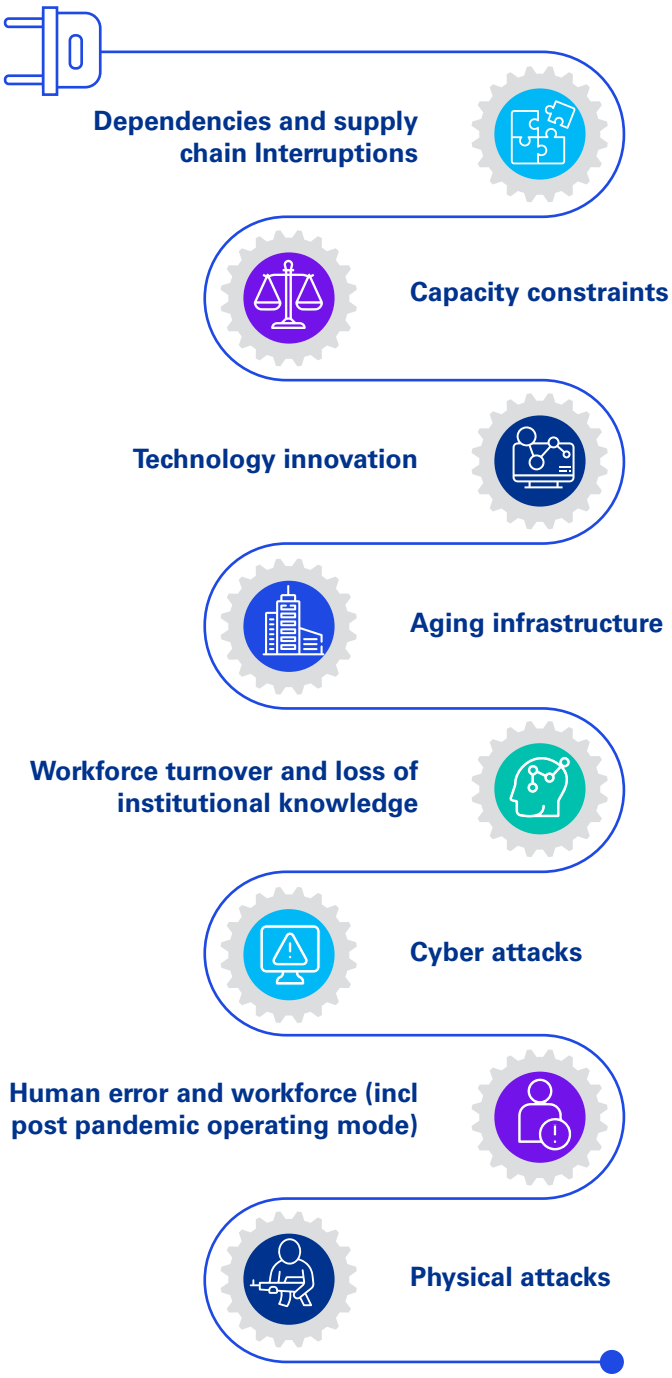


[2] National Centers for Environmental Information, Billion-Dollar Weather and Climate Disasters, Accessed 10 June 2022

[3] US Energy Information Administration, US electricity customers experienced eight hours of power interruptions in 2020, November 2021

[4] Bloomberg, Climate Change Turned Up India's Heat. But by How Much?, May 2022

Operational threats



Decentralization and digitization

Grids are becoming more distributed, with swathes of smaller, localized sources, creating a hybrid mix of conventional/nuclear and, increasingly, renewable energy from small hydro, biomass, biogas, solar, wind and geothermal.[5] It's quite a headache to orchestrate this complex web of players, in order to maintain system integrity.

At the same time, digitization brings greater automation and sophistication to control systems, integrating operations and IT, with growing dependence on an external cloud network and as-a-service providers. With such an interconnected backbone, a single failure can have multiple consequences and potentially shut down the whole facility.

Any incident instantly exposes the many interdependencies in society, where one outage has a chain reaction impacting telecommunications, industry, transport and water. For example: if there is no mobile network or internet, it's harder to contact engineers and other repair personnel. And if electric power is out and gas stations are not working, these same people cannot drive to reach the points of damage. Coping with surges is a further challenge when many players are involved in the grid, as the customer-facing providers seek to distribute energy from multiple locations.

As P&U providers transition to digital enterprises, where every piece of equipment, including hardware, IoT sensors, and personal devices are connected, and where many

[5] Power Grid International, A look towards the future: Integrating DERMS and ADM, May 2019

third parties are involved in transmission and billing, the threat — and the subsequent impact — of cyberattack has risen dramatically. Since the pandemic, the acceleration of hybrid working has increased awareness of how attackers can hack into systems on insecure networks. Deteriorating relations with other countries adds another layer of threat.

P&U organizations have often been targeted by cybercriminals and nation states (sometimes both working in tandem) to disrupt enemies' critical national infrastructure. Cyber weapon Stuxnet was believed to have been co-developed by Israel and the US to attack Iranian nuclear facilities, although both Israel and Iran deny this.[6] Stuxnet took out SCADA systems within critical Iranian nuclear facilities.[7]

Another example is NotPetya, which experts claim has been aimed at Ukraine.[8] McAfee states, "…this variant was designed to spread quickly," targeting "complete energy companies, the power grid, bus stations, gas stations, the airport, and banks."

Organizations may not be directly targeted but end up collateral damage, as malware released 'into the wild' exploits their vulnerabilities. Stuxnet may well have had a specific target, but the code used to develop the original malware has now been enhanced and can be used to attack a much broader audience across sectors and geographies.

NotPetya may have had the energy sector in its sights, and potentially Ukraine. Still, it has impacted many global organizations, including the aircraft Antonov in Ukraine, logistics giant Maersk, and Russian oil producer Rosneft.[9]

It's not uncommon for hostile hackers to follow up a cyberattack with a physical attack. The attack surface is vast because of the enormous networks of stations, pylons, and other facilities. The lack of a reserve power source makes it even more challenging to recover by getting a generator back up and running.

Aging assets and workforce

In an asset-heavy sector, cost-effective replacement and maintenance are constant factors. Climate change has reminded P&U companies how easily some equipment can become damaged. In the case of forest fires, in particular, fallen power towers and lines can be responsible for loss of life and livelihood, resulting in hefty fines or even criminal action against executives for failing to adopt suitable preventative measures.

Without the right people and skills, P&U networks may struggle to achieve the levels of continuity that customers demand. As the older generation of workers approaches retirement, it's vital to attract new talent into the sector and pass on the decades of experience of older generations. And as roles become ever more digital, technological capabilities become essential in combination with automation.

"Stuxnet may well have had a specific target, but the code used to develop the original malware has now been enhanced and can be used to attack a much broader audience across sectors and geographies."

[6] The New Yorker, World War Three, By Mistake, December 2016

[7] Foreign Policy, Stuxnet's Secret Twin, November 2013

[8] Wired, What is the Petya ransomware spreading across Europe? WIRED explains, July 2017

[9] BBC, Global ransomware attack causes turmoil, June 2017

Building a resilience framework and culture

As they strive to build safe and robust organizations that can provide 24/7, uninterrupted services to public and private organizations and citizens, P&U companies are treating resilience as a board-level imperative.

The UK has a National Resilience Strategy[10] designed to cope with extreme weather, terrorism, pandemics, cyberattacks, geopolitical instability, and accidents. The country's National Grid adopts a 'Whole Systems' approach.[11] And in the US, the National Institute of Standards and Technology (NIST) provides a technical basis for improved design, construction, operation, and maintenance of buildings and infrastructure systems.[12]

Integrated resilience framework

Define scope and understand stakeholders needs and requirements

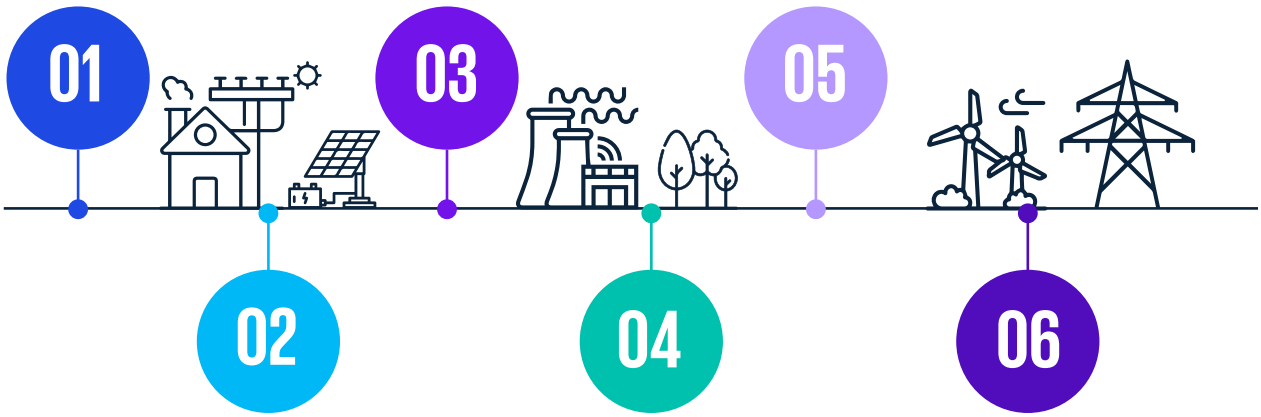
- Consider threat and subsystems of concern
- Define stakeholder expectations

Develop and assess resilience mitigations

- Develop resilience mitigations and alternatives
- Assess impact on resilience risk
- 4 R: Redundancy, Resistance, Response and Recovery

Implement and measure

- Develop after-action reports and lessons learned
- Metrics and KPIs



Risk assessment to determine threat susceptibilities and vulnerabilities

Develop resilience plan

Mitigation portfolio development

Mitigation funding

Response and recovery

System goal

Maintain energy availability to customer and consumers

[10] UK Government, National Resilience Strategy: Call for Evidence, July 2021

[11] National Grid, Our Whole System approach, March 2021

[12] National Institute of Standards and Technology, Resilience, accessed June 2022

A resilience strategy should exhibit the following characteristics:

Extreme weather event modeling

P&U planners should improve their scenario planning to cope with climate change threats. Historical events are no longer a reliable predictor of the future, so models must take in more real-time data and use innovations like digital twins to forecast the likelihood and the severity of the impact on the infrastructure and interdependent services.

Preparedness of equipment and people

Preparedness is equally critical, investing in newer, more robust infrastructure, stocking up on inventory, and having extra staff and contractors available on call to make repairs as quickly as possible. Procurement professionals may have to reconsider their just-in-time ambitions, given an outage's enormous potential cost and inconvenience. This involves cost-benefit decisions: over-prepare and you will add significantly to expenses; under-prepare and you risk unacceptable outages, unhappy customers and massive repair bills. Equally, certain types of inventories like super grid transformers are so specific to different parts of a grid that it's impossible to hold every stock item.

Hardening

There are many steps P&U companies can take to make their physical infrastructure more resilient, such as installing stronger poles, undergrounding overhead lines, trimming trees, and raising substations above predicted flooding levels. Longer-term scenario planning can guide the thinking to consider likely weather conditions in the coming decades.

Investments in replacement and maintenance must balance upfront costs now and potentially significant expenses later to remedy the damage. Studies tend to show that upgrades are many times cheaper than repairs — a US review concluded that every US$1 invested in disaster mitigation or 'hardening' was found to avoid US$6 in rebuilding costs.[13] In one instance, by installing new transformer monitors, a company prevented an outage for 15,000 customers, saving approximately US$1 million in restoration charges.[14]

There's growing interest in predictive maintenance, using sophisticated sensors, drones and other IoT, which, combined with advanced analytics, can help determine when equipment may fail, initiating proactive action. Cloud-based, predictive platforms use AI and automation to constantly improve their ability to spot asset defects and avoid equipment downtime. And by combining these with accurate extreme weather forecasts, companies can be better prepared.

One way to build resilience is through redundancy, so that different transmission lines can operate independently of each other; if one fails, the others continue to work. Monitoring is essential to this approach, detecting any operational problems — such as cyberattacks or mechanical failure — and enabling systems to isolate these to 'fail safely' to avoid broader system disruption.

Distributed generation builds more alternative sources into the grid, including an increasing usage of microgrids. Energy storage can increase resilience, providing an alternative energy source, acting as both load and generator.

Cyber security

And, of course, cyber defense is becoming a big priority, with an urgent need to establish cyber-aware cultures and strict entry protocols. It's also vital to identify and nullify potential threats and restore systems should they come under attack. Some are sweeping out old legacy technology and moving to the cloud to remove as many potential vulnerabilities as possible.

Creating a resilience culture

Finally, embedding knowledge in the system can help avoid 'key person' risk where organizations depend on individuals' unique abilities. Strategic workforce planning identifies the skills and leaders needed and the working environment that will appeal to a new, diverse workforce. Investing in technical skills training and building new routes to recruitment and contractors/gig economy workers, will likely be crucial.

[13] Federal Insurance and Mitigation Administration, Natural Hazard Mitigation Saves Interim Report, June 2018

[14] T&D World, Ushering in the Next Era of Grid Modernization, December 2021

Investing in a trusted and reliable future

Resilience doesn't just keep the lights on; it builds trust and drives competitive advantage.

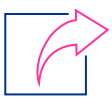
In a resilience-focused organization, leadership has clear accountability for protecting service delivery, supported by robust data insights that can inform investment in longer-term resilience, meet evolving regulatory requirements, and help ensure swift preventative action in the event of failures. Resilience planning has three main areas:

Prepare

- Enterprise service management
- Resilience control frameworks
- Tolerance and scenario management

Assess

- Non-stressed service resilience assessment
- Service threat management assessment
- Stressed service resilience assessment



Action

- Reporting, solutions, and investment appraisal
- Service enhancement
- Recovery planning and management

How KPMG can help

KPMG power and utility professionals have extensive experience in building more robust organizations and can help you:

- Make resilience and trust foundations of your organizational strategy and value proposition
- Be agile and flexible in maintaining business outcomes after disruptive events
- Keep your business connected internally and externally, before and after disruption
- Make your resilience data-driven and tech-enabled to generate timely insights, reduce costs and improve scalability

This should give you clear visibility and control of services, resources and risks — leading to more assured stability of services in times of disruption. It can also support the business, customers, and financial markets so that resilience can become a critical competitive advantage and a driver of trust.

About the authors

Ali Abedi
Senior Manager, Cyber Resilience — Global Cyber SGI
KPMG in the UK
E: ali.abedi@kpmg.co.uk

Ali leads KPMG in the UK's Cyber Resilience capability. With over 25 years of experience designing, developing and implementing resilience solutions across multiple industry sectors, including power and utilities, Ali has built cyber resilience solutions for influential organizations with an extensive global footprint ensuring solutions cover the impact of cyber threats by country and region globally. These solutions have been developed for operational, tactical and strategic response capabilities across major organizations, ensuring that the whole organization can respond to major cyber events appropriately.

Cassandra Hogan
National Industry Leader, Energy & Natural Resources
KPMG Australia
E: cjhogan@kpmg.com.au

Cassandra's passion for the energy industry started early in her career with her first job in a large utility call center. This gave Cassandra an enormous appreciation of customer focus and grounded her in the importance of 'rolling up your sleeves and delivering on commitments. What followed was 16 years in a diverse range of roles from frontline operations, strategy, merger integration and business transformation in a period of significant change in the energy sector.

As National Industry Leader for Energy & Natural Resources, Cassandra brings an entire firm perspective to problems, aware that technical solutions are only as good as their implementation ability. Cassandra is also a mentor to women in the energy and resources sector.

Onur Karakus
Senior Consultant, Cyber Strategy & Risk
KPMG in the Netherlands
E: karakus.onur@kpmg.nl

Onur is a business resilience risk management specialist who has 10-plus years of experience in the field. Throughout his career, he has led and delivered multiple business continuity projects dealing with cyber and business interruption risks. Onur has built extensive experience in business resiliency, particularly in the energy sector, helping industry leaders to formulate and implement business continuity strategies. He helps organizations perceive disruptive risk environments, manage risks and prepare the best possible response strategies with the help of technology and cyber security.

Ramsay Sawaya
Managing Director, Power & Utilities Strategy
KPMG in the US
E: ramsaysawaya@kpmg.com

Ramsay has 30 years of service in electric and gas utilities. His expertise is in leading utility transformation in ESG, risk and resilience, and asset and investment management to help electric and gas utilities navigate a changing business environment. He has supported the development of the strategic direction and assessed and implemented leading practices in risk, resilience, and asset management across the industry.

05

Incident readiness: a playbook for your worst day

Being prepared for a cyber incident can minimize critical power and utility infrastructure disruption.

By: Jason Haward-Grau,
Lars Jacobs, and Maliha Rashid

Over the last couple of years, the cyber threats to power and utilities (P&U) organizations have risen significantly, notably from increasingly sophisticated ransomware and malware attacks. Malware, in particular, can spread rapidly, disrupting processes, stealing data, threatening safety and cutting vital services to government, business and consumers.

More than one-third (37 percent) of organizations have been hit by ransomware in the past year alone,[1] and a quarter (26 percent) have been forced to close some operations.[2] Incidents also have more severe consequences, with average downtime rising from 5 to 26 days[3] in recent years and average ransomware payments increasing by 144% since 2020.[4]

The P&U sector faces a constant and growing risk, from a 2021 attempt to poison a city in Florida by hacking into the water treatment system[5] to a suspected state-sponsored cyberattack on India's power grids in 2022 via IoT devices and cameras.[6]

The operational technology (OT) estate is especially vulnerable, with nine out of ten organizations experiencing at least one system intrusion in the last year.[7] A similar proportion admits it has limited-to-no visibility into its industrial control system (ICS) environments due to their age and legacy technology.[8]

Since the invasion of Ukraine, Russian hackers have been circling vital US and other nations' energy infrastructure, searching for opportunities and weak points in digital systems to steal sensitive information or disrupt operations.[9]

Unlike IT, which tends to have a 3–5 year life cycle, many P&U OT estates run on old and often unsupported software and hardware. With digital transformation making OT increasingly IT-dependent, there is a growing attack surface that hackers can and will seek to exploit. In addition to traditional players, the threat extends to a host of smaller startups selling electricity and gas and supplying their meters. Many of these companies are essentially marketing and customer service operators with relatively immature cyber security.

In a digital world, where everything is connected, grid shutdowns can bring public services, businesses and homes to a standstill. Not everyone has a backup generator, and a

Growth of ransomware

90% of organizations had at least one system intrusion[7]

37% of organization said they were victims of ransomware[1]

26% said the attacks caused a suspension in operations[2]

26 days average downtime[3]

US$2.2M average ransom demand[4]

1 Sophos, The state of Ransomware 2021, April 2021
2 Cybereason, Ransomware Attacks and the True Costs to Business, Dragos 2020 ICS Cybersecurity Year in Review
3 Coveware, Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting, May 2022
4 Unit 42, 2022 Unit 42 Ransomware Threat Report, March 2022
5 CNN, Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says, February 2021
6 Business Standard, Suspected Chinese hackers collect intelligence from India's power grid, April 2022
7 Fortinet, 2020 State of Operational Technology and Cybersecurity Report, April 2021
8 Cybereason, Ransomware Attacks and the True Costs to Business, Dragos 2020 ICS Cybersecurity Year in Review
9 The Texas Tribute, Texas power grid, energy sectors facing elevated Russian cyber threats during war in Ukraine, March 2022

power outage instantly exposes our growing dependence on electricity across every part of daily life. Connectivity also carries the threat outside the organization to millions of customers-via IoT devices like smart meters in homes, and online access to billing accounts-opening up opportunities for phishing and other forms of unauthorized entry into P&U systems.

Aware of these dangers, regulators are exerting more significant pressure on companies to demonstrate secure cyber defenses. The EU's Cyber Resilience Act seeks to establish a baseline of resilience across industries, with a strong focus on critical P&U infrastructure.[10] In the US, the Transport Security Administration (TSA) Security Directives (published in the wake of a 2021 cyberattack on Colonial Pipeline) requires electric and gas utilities to assess all their assets to ensure they meet new, higher safety standards and produce clear incident readiness plans.[11]

> "In addition to traditional players, the threat extends to a host of smaller startups selling electricity and gas and supplying their meters."

Building incident readiness 'muscle memory'

A robust cyber security culture can significantly reduce the chance of an attack, but P&U organizations should also be ready should an incident occur. Incident readiness is about developing a playbook for that 'worst case' scenario, mitigating vulnerabilities in advance, and documenting a plan to respond quickly and decisively. Through training and exercises, it's possible to build up invaluable 'muscle memory.'

Cyber resilience consists of three key stages: readiness, response, and remediation — the latter to address root causes and hopefully prevent a re-occurrence.

Readiness is the foundation of resilience, with a robust plan defining the roles and responsibilities of different stakeholders and the necessary actions to respond and recover swiftly to help minimize the impact on the organization and its customers. Plans should be in both secure electronic format and hard copy to ensure access should systems go down. The three components of a readiness plan are:

- **People**, establishing a chain of command that names the critical decision-makers, the skills they should possess, and any training needed to fill gaps.
- **Processes** — specific incident response steps for different scenarios, external and internal communications (including legal obligations), and a clear path to business as usual. P&U OT applications typically have less robust backup and recovery capabilities than IT systems, so these need to be strengthened and given explicit control permissions.
- **Technology** is a significant component of the plan, outlining the data needed, the steps and processes to locate and gather this information, and tools for analyzing what happened and facilitating a fast recovery.

A plan should consider the broadest range of adverse outcomes, including disruption to power generation or fire extinguishing systems and other ripple effects. Maintenance windows (time needed to fix problems) may be affected by an attack, so it's vital to carry out testing and safety checks.

Working through different scenarios can help organizations figure out the impact of attacks on vital operational assets like data storage facilities or human management interfaces — which could stop power from being generated. If such assets are temporarily paralyzed, switching to the training control room is an option, but this could also go offline.

[10] European Commission, Cyber resilience act — new cybersecurity rules for digital products and ancillary services, March 2022

[11] Burns McDonnell, Cybersecurity Directives Require Quick Action by Electric/Gas Utilities, March 2021

Doing the drill

Simulations or 'tabletop' exercises are a regular feature of mature cyber security culture, helping P&U organizations improve their ability to detect network attacks earlier, enabling faster containment to prevent escalation. The drill should identify gaps in detection software and intelligence gathering, to keep on top of potential threats worldwide. And by showing up more clearly the links between physical hazards and cyber issues, it will build a greater appreciation of the broader impact of an attack and help reduce the risk of an incident occurring in the first place.

In a typical exercise, a facilitator walks staff through a tailored cyber incident, tasking the group to evaluate options and make decisions at crucial moments, exposing key individuals to real-life challenges to get operations back on track in the shortest possible time. This improves readiness, gets the players familiar with their responsibilities, and uncovers operational weaknesses.

By bringing together stakeholders — like the CIO, CISO, Head of OT Operations, or an OT shift manager — who don't usually interact, incident readiness drills expose people to different ways of looking at the organization. OT staff tend to be concerned with operational safety, process optimization and reliability, while their IT counterparts think more about confidentiality, availability, and integrity. Bridging this mindset gap can help teams collaborate more effectively and think through practical questions that may never be discussed until an incident occurs, such as: how will we all connect? And where/how will we meet?

A robust and underlying security culture can make a difference when spreading cyber awareness and responsiveness. Many water and energy providers, including solar, wind, biomass, gas, and coal, have traditionally had relatively relaxed health and safety environments, without rigid restrictions save for the generator area. Now that cyber has become a recognized threat, these organizations must build awareness and encourage good habits.

Accessing the resources you need

Cyber attackers are becoming more active, and ransomware and malware incidents are increasing in both frequency and severity. P&U organizations may not be able to prevent every attack, but they can improve their incident readiness.

Armed with a tried and tested playbook, P&U organizations can respond at pace, with a documented set of tasks, a transparent chain of command, and knowledgeable individuals with the muscle memory to mobilize and close the threat down as quickly as possible, protecting the safety of all employees and keeping vital national infrastructure up and running.

However, an incident readiness plan is only as good as the people that operate it, so organizations need a strong focus on training and resourcing. This should ensure that relevant workers are skilled and drilled in containment and recovery, with the plan leader able to locate and deploy the appropriate individuals quickly. Given the enormous demands on staff during an incident — with the IT team often working around the clock — tiredness and mistakes can creep in, so it's essential to have resources in reserve to take over.

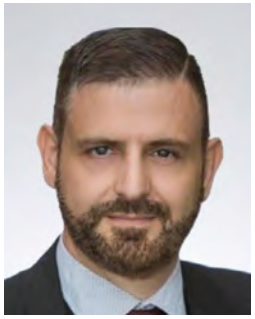
Finally, P&U organizations should recognize that even the most efficient incident readiness plan has room for improvement. That's why an external perspective can be invaluable in building resilience. A skilled third-party specialist can guide the readiness team through the various steps and carry out an incident readiness assessment, with recommended actions to overcome gaps.

How we can help

At KPMG, we have carried out multiple incident readiness assessments and tabletop exercises for P&U and industrial businesses. We bring a wide range of highly qualified and experienced team members into incident readiness, from security and penetration testers to operational consultants, cyber readiness experts and recovery practitioners who have been directly leading recovery efforts for impacted clients. KPMG was delighted to be recognized as a 'Leader' in Worldwide Incident Readiness Services by IDC Marketscape in 2021.

Clients particularly value our multi-sector view. Too often, businesses are contained within their industry bubble and have limited awareness of best practices in other sectors that they may be able to import and apply. KPMG professionals have worked on incident readiness and simulations across many industries, including financial services, automotive, chemicals and manufacturing.

About the authors



Jason Haward-Grau
Advisory Managing Director, Cyber Security Services
KPMG in the US
E: jhawardgrau@kpmg.com

Jason Haward-Grau is a leader in KPMG in the US's Cyber Security practice, with a proven track record as a cyber executive in multiple industries with more than 20 years of experience developing, delivering and sustaining cyber security strategy, programs and operations across energy, luxury fashion and critical infrastructure sectors.

Lars Jacobs
Advisory Senior Manager, Cyber Security Services
KPMG in the Netherlands
E: jacobs.lars@kpmg.nl

Lars leads KPMG's Cyber Response practice in the Netherlands. In that role, he helps KPMG clients during the crisis phase of a cyber security incident and brings the knowledge and experience to them to prepare themselves effectively.

Maliha Rashid
Data Privacy Lead, Digital & Innovation — Cyber
KPMG Lower Gulf
E: mrashid5@kpmg.com

Maliha is a Director within KPMG Lower Gulf's Digital & Innovation practice. She has over 17 years of experience in cybersecurity and data privacy across France and the Middle East. She has led award-winning cyber security and data protection transformation programs in Europe and the UAE. Before joining KPMG, Maliha was the Head of Cyber security Risk at a major airline. Prior to this, she worked with Big Four consulting firms for over 12 years in France and more recently in the Middle East, delivering cyber security engagements across various sectors, including financial services, industry, luxury and telecommunications.

06

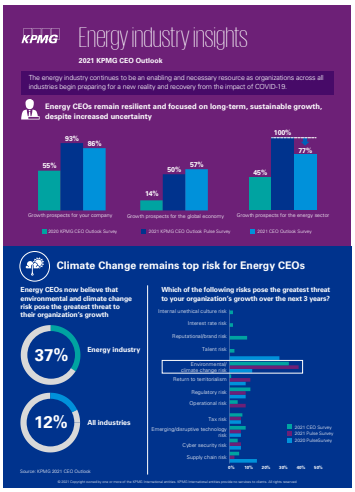
KPMG's Global Energy Institute

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 Power & Utilities and Oil & Gas industries. The GEI helps shed light on key topics ranging from upstream volatility, midstream constraints, industry consolidation, shifting customer demands and new technologies, alternative and renewable energy, smart grid technology and transformation, and evolving regulatory and statutory requirements, as well as financial reporting and tax updates.

The GEI interacts with its over 40,000 members through various channels, including webcasts, publications and white papers, podcasts, events, and quarterly newsletters. The institute works with member firm clients, external partners and the global KPMG network of energy experts to analyze the most pressing challenges facing the industry and develop 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 industry trends 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 energy industry, become a member of the KPMG Global Energy Institute today by visiting home.kpmg/energy.



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 cyber security consulting market leader. Our cyber security capabilities are truly global, with over 3,200 information security professionals working in KPMG firms across the world.

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

> "The GEI interacts with its over 40,000 members through various channels, including webcasts, publications and white papers."

Strategy and 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 a changing environment.

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 is rated as the most familiar energy and resource consulting brand on a list of the world's top 15 consulting organizations. KPMG also earned top marks for quality from 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 scores from 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 its 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, Colleen King, Arun Mani, Michael Morihovitis, Michael Quigly, and Peter Valentin.

Contacts

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

Valérie 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

Jorn De Neve
Partner, Head of Energy & Natural Resources
KPMG in the Belgium
E: jdeneve@kpmg.com

Magali Vercammen
Energy & Natural Resources Sector Lead
KPMG in Belgium
E: mvercammen@kpmg.com

Philip Jeandarme
Energy & Natural Resources, Technology Lead
KPMG in Belgium
E: pjeandarme@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg/pluggedin

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: Plugged In
Publication number: 138193-G
Publication date: June 2022