WORLD
ENERGY
COUNCIL

Cyber challenges to the energy transition

In Partnership with Marsh & McLennan Companies
and Swiss Re Corporate Solutions

WORLD ENERGY COUNCIL
The World Energy Council is the principal impartial network of energy leaders and practitioners promoting an affordable, stable, and environmentally sensitive energy system for the greatest benefit of all.

We are the UN-accredited global energy body, representing the entire energy spectrum, with member organisations in over 90 countries.

Further details can be found at www.worldenergy.org and @WECouncil.

Published by the World Energy Council 2019

World Energy Council
Registered in England and Wales
No. 4184478

VAT Reg. No. GB 123 3802 48

Registered Office
62–64 Cornhill
London
EC3V 3NH
United Kingdom

TABLE OF CONTENTS

AN EXPANDING DIGITAL FOOTPRINT

The energy sector is experiencing a transformation. Major shifts in global supply and demand on almost every front are creating both fresh opportunities to explore and new threats to manage. This transition is also being shaped by digitalisation of the industry. The adoption of intelligent, sophisticated technology, including artificial intelligence (AI) for control and monitoring systems, is enabling new business models and more efficient asset management. New synergies are being realised through linking operational, information technology (IT), and communication systems within organisations and across the energy supply chain as the sectors' digital footprint expands. (See Exhibit 1.)

Digitalisation and the development and transformation of energy supply chains are at the core of many government and businesses priorities. As can be seen from the Council's 2019 World Energy Issues Monitor, it is one of the top ranked uncertainties in terms of impact for energy leaders. (See Exhibit 2.) Responding to the effects of digitalisation is closely linked to other issues, such as connected infrastructure or the industrial "Internet of Things," blockchain, data and artificial intelligence, decentralised systems, and artificial intelligence (AI), energy efficiency, and cyber threats.

The transforming energy sector requires new, agile risk management approaches to match its evolving risk profile and ensure it continues to be effective and reliable given the critical role it plays in every country's infrastructure.

Exhibit 1: Energy sector's expanding digital footprint

Downstream companies use supply-demand matching smart grids and complex algorithms constantly adjust flows helping companies improve margins and identify necessary predictive maintenance.

Oil and gas companies depend on data networks to track data from thousands of oil and gas wells and thousands of kilometers of pipelines, manage facilities, and interpret operating conditions.

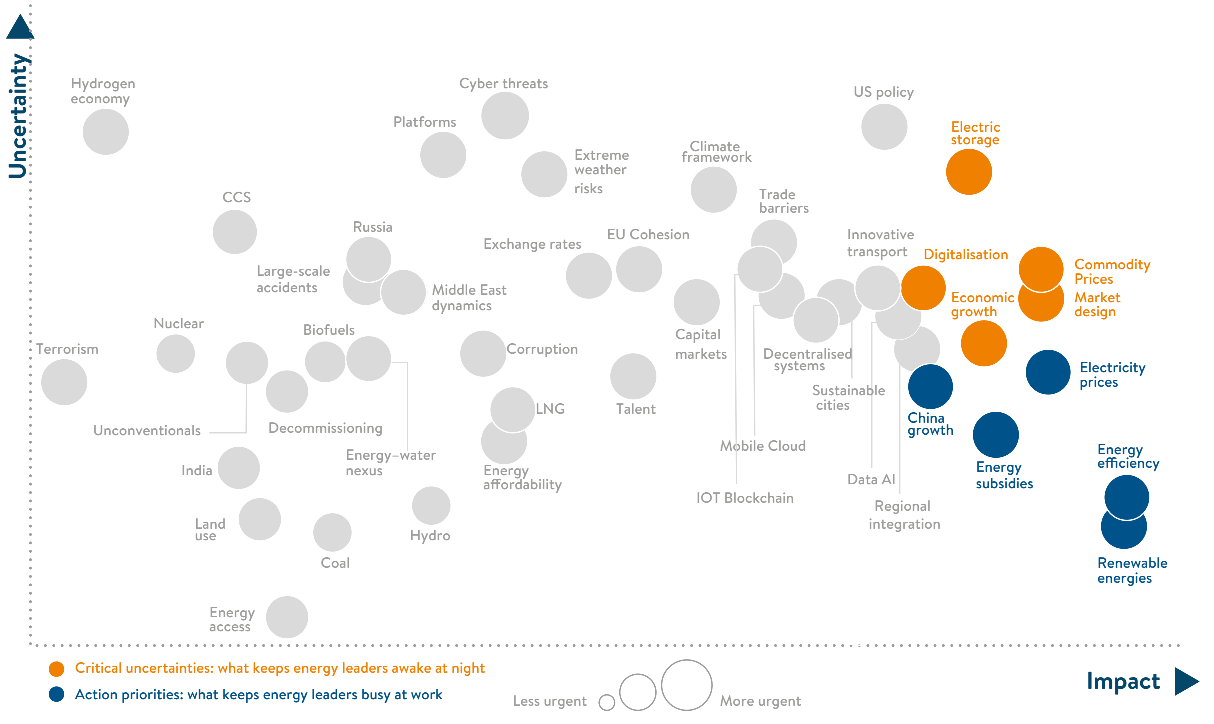
Upstream companies use digital technologies for reservoir modelling, drilling resource dispatching, production optimisation, and more.

Electric transmission companies depend on automated controls to run their networks.

Utilities rely on data networks to manage complex combinations of centralised grids and decentralised resources to analyse and efficiently meet customers' needs on a minute-by-minute basis.

Source: Marsh & McLennan Companies

Exhibit 2: Top ranked issues in World Energy Issues Monitor



Source: World Energy Issues Monitor, World Energy Council, 2019

INCREASING RESILIENCE AND VULNERABILITY

In many aspects, the resilience of the energy sector is greatly increased by digitalisation as it enables the use of a complex and widening array of decentralised resources, improved efficiency, and enhanced abilities to detect threats, thereby increasing operational accessibility, productivity, sustainability, and safety.

At the same time, digitalisation presents new challenges. For example, cyber or digital disruption risk can affect every operation within a power plant especially with the increased use of connected industrial devices and automated controls. The pace of digitalisation in the energy sector may potentially outpace cyber defence and digital management capabilities, resulting in greater exposure to risk.

The digital energy sector includes five factors that increase its vulnerability to digital disruption or cyber threats:

1. The rapid pace of innovation;
2. Technological complexity;
3. Data sharing and interconnectivity;
4. Rising cyberattack sophistication; and,
5. The sector's attractiveness as a cyber target.[1]

[1] Advancing Cyber Risk Management: From Security to Resilience. FireEye and Marsh & McLennan Insights, 2019

The energy sector's digital backbone is vulnerable to failures from a range of sources. These include non-malicious human errors or software failures in systems developed within the sector's increasingly complex supply chain or operations, insider threats from disgruntled employees, malicious external cyberattacks, and even the impact of space weather or geomagnetic storms.[2] A wide range of malicious external actors often target power grids motivated by financial goals, such as ransom ware or intellectual property theft, or sometimes they aim to cause broader economic and social harm. In addition, like all organisations, energy companies can be collateral damage from an attack not directed at a specific company, such as fast-spreading malware like NotPetya attacks in 2017.

Interconnectivity and complexity create vulnerabilities to malfunction or sabotage that can cascade across the energy sector and impact the broader economy. This was highlighted by the recent widespread blackout impacting approximately 48 million people in Argentina and Uruguay. The cause is still unknown, but the complexity of the system is such that "...just milliseconds passed from the destabilisation of the grid to the power being cut."[3] Trains and subways were halted, traffic lights did not function, and the water company's distribution system was compromised.

[2] Space weather or geomagnetic storms, such as solar coronal mass ejections that release electromagnetic pulses, can impact the electrical power grid including high-voltage transmission lines, transformers transmission distribution centers, and fuses.

[3] Millions were left without power in Argentina and Uruguay after an 'extraordinary' system failure. How did it happen?, Time Magazine, June 17, 2019

Complexity is also a factor in the oil and gas sector. As companies have streamlined their operations, supply chains are becoming more integrated and interdependent. If one part of a supply chain is interrupted, it carries the potential for consequences across the entire chain. This was demonstrated by a cyberattack on seven US pipeline operators in 2018 that impacted third-party electronic communications systems and the ability to issue timely bills to customers.[4]

The potentially cascading impact of malicious cyberattacks on critical infrastructure is a rising concern for the sector and governments. And with good reason. The frequency and severity of cyber incidents in the power sector are increasing. Phishing remains the most common means of attack, but actors are also deploying a more extensive range of methods such as credential theft, ransomware, and advanced persistent threat.[5] The number of known attack groups increased from 140 in 2018 to 155 in 2019.[6] (See Exhibit 3.)

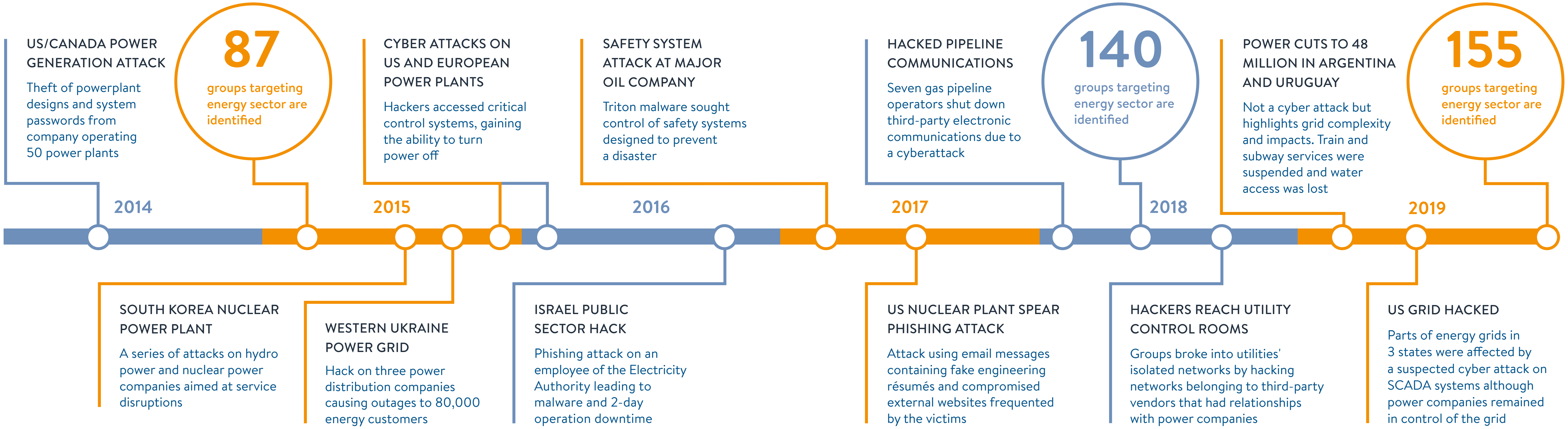
Overall, the rising vulnerability to digital disruptions or cyberattacks pose threats to business continuity and the bottom line. In addition, concerns that a cyberattack could cross over to the

[4] Cyberattack bleeds into utility space with billing delays, Houston Chronicle, April 5, 2018

[5] Advancing Cyber Risk Management: From Security to Resilience, FireEye and Marsh, 2019

[6] ISTR 2019: Targeted Attack Groups Increase Despite Growing Risk of Exposure, Symantec, 2019

Exhibit 3: Cyber incidents increasing in both frequency and impact



US/CANADA POWER GENERATION ATTACK

Theft of powerplant designs and system passwords from company operating 50 power plants

87 groups targeting energy sector are identified

CYBER ATTACKS ON US AND EUROPEAN POWER PLANTS

Hackers accessed critical control systems, gaining the ability to turn power off

SAFETY SYSTEM ATTACK AT MAJOR OIL COMPANY

Triton malware sought control of safety systems designed to prevent a disaster

HACKED PIPELINE COMMUNICATIONS

Seven gas pipeline operators shut down third-party electronic communications due to a cyberattack

140 groups targeting energy sector are identified

POWER CUTS TO 48 MILLION IN ARGENTINA AND URUGUAY

Not a cyber attack but highlights grid complexity and impacts. Train and subway services were suspended and water access was lost

155 groups targeting energy sector are identified

SOUTH KOREA NUCLEAR POWER PLANT

A series of attacks on hydro power and nuclear power companies aimed at service disruptions

WESTERN UKRAINE POWER GRID

Hack on three power distribution companies causing outages to 80,000 energy customers

ISRAEL PUBLIC SECTOR HACK

Phishing attack on an employee of the Electricity Authority leading to malware and 2-day operation downtime

US NUCLEAR PLANT SPEAR PHISHING ATTACK

Attack using email messages containing fake engineering résumés and compromised external websites frequented by the victims

HACKERS REACH UTILITY CONTROL ROOMS

Groups broke into utilities' isolated networks by hacking networks belonging to third-party vendors that had relationships with power companies

US GRID HACKED

Parts of energy grids in 3 states were affected by a suspected cyber attack on SCADA systems although power companies remained in control of the grid

Sources: Marsh & McLennan analysis

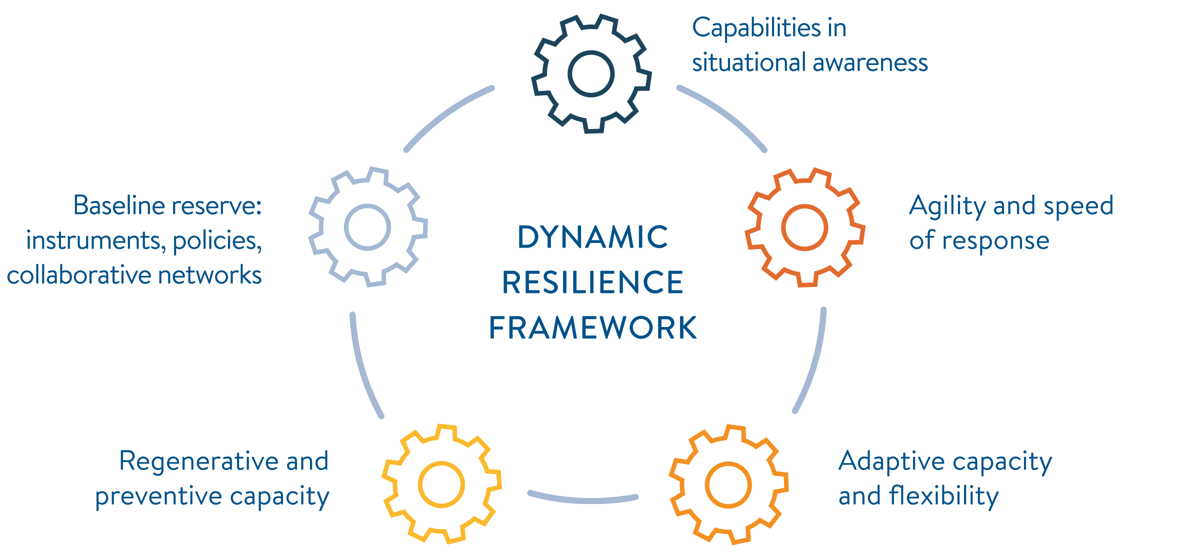
physical world raise real concerns about property damage and bodily injury. In a recent survey by Marsh in partnership with Microsoft, 76% of energy executives cited business interruption as the most impactful cyber loss scenario for their organisation.[7] The losses can include direct costs such as loss of revenue due to operational/productivity disruptions, costs associated with restoring operations and improvements to cybersecurity defenses, regulatory fines, and legal liability, as well as indirect costs such as regulatory fines and reputational damage.

Contagion effects and the interconnectedness of energy and power systems raise many questions and challenges for energy companies, regulators, policy makers, and stakeholders as they try to grasp the potential scale of an event and determine the best approach to risk management.

THE NEED FOR DYNAMIC RESILIENCE

The transforming characteristics of the energy sector, along with an evolving vulnerability profile, require an step-change in risk management with a focus on creating dynamic resilience capabilities. These include an agile and adaptive response framework focused on regeneration and rapid recovery.[8]

Exhibit 4: Dynamic Resilience Framework


Capabilities in situational awareness
Agility and speed of response
Adaptive capacity and flexibility
Regenerative and preventive capacity
Baseline reserve: instruments, policies, collaborative networks
DYNAMIC RESILIENCE FRAMEWORK

Source: World Energy Council

[7] Marsh-Microsoft Global Cyber Risk Perception Survey, 2017

[8] Managing Energy Transition Through Dynamic Resilience, Martin Young and Angela Wilkinson, World Energy Council, 2018

In a rapidly evolving sector, an approach of static policies or protocols to known risks will not be an adequate or efficient risk management strategy. Put differently, as it becomes increasingly difficult to control all risk drivers, the emphasis on response and recovery is heightened.

The World Energy Council's Dynamic Resilience framework contains five criteria designed as a checklist to help energy actors strengthen resilience planning efforts (see Exhibit 4). Dynamic resilience adopts a stance of continuous learning, rather than the conventional risk-based approach of reducing uncertainty to enable control of the future. The emphasis is on anticipating, recognising, and addressing disruptive changes, which are characterised by novelty and uncertainty, by triggering improvisation and accelerating experimental, interactive, and collaborative responses. By accelerating systems integration, resilience is no longer just about returning single assets or components to full operation after a disruptive event, but part of a coordinated approach to ensure the optimal recovery of the energy system as a whole.

APPLYING THE DYNAMIC RESILIENCE FRAMEWORK

Energy companies need to ensure their risk management and response practices evolve to be fit for a digitally-controlled environment as compared to a physically controlled environment. For example, applying decentralised resilience to standards and rules so that intelligent systems stop connecting and lock into safe mode when abnormalities are detected.[9] Applying the concept of dynamic resilience to digital security would include the following:

BASELINE RESERVES – INSTRUMENTS, POLICIES, AND COLLABORATIVE NETWORKS

This involves the systems, policies, and processes in place to strengthen resilience. For digital resilience, this would involve a comprehensive cyber risk management framework that includes regularly tested incident response plans. Organisations should also consider links to networks that strengthen resilience, such as the ability to tap into mutual aid schemes to expand the pool of specialist experts in a crisis. There should be stakeholder, supplier, and customer engagement plans to provide timely updates to key parties (e.g., the capacity to set up customer hotlines).

CAPABILITIES IN SITUATIONAL AWARENESS

This is the ability to monitor, understand, assess, and continuously refresh the landscape of current and evolving digital and cyber risks, exposures, and potential impact on the organisation and understanding the scope for cascade within and beyond the sector. It includes quantitative and qualitative information, including assessments of potential cyber risk exposure and potential business impact (e.g., power outage and impact on revenue, net fuel, or energy margin basis) to help key decision-makers determine how to best allocate cyber risk management resources and focus these resources in a crisis. Further, as part of a pre-crisis preparation, organisations should map what information would be most useful (and how it should be collected, processed, and presented) to decision-makers and stakeholders (e.g., well-designed and updated cyber risk dashboards).

[9] Are Manufacturing Facilities As Secure As Nuclear Power Plants?, Claus Herbolzheimer and Richard Hell, Oliver Wyman, www.oliverwyman.com

AGILITY AND SPEED OF RESPONSE

This is the capability to quickly assess a situation and implement the most effective mitigation or adaption policy. It includes rapid prioritisation setting and coordination with key stakeholders. One of the most important benefits of an efficient event response system is the ability to react swiftly to a crisis and thereby decrease the severity of an event and lessen the reputational impact. Looking at the impact of cyberattacks on share performance across sectors, research has found that the immediate transparency on the issue with stakeholders, backed by high quality and honest communication, has served to support a positive increase in share performance.[10]

ADAPTIVE CAPACITY AND FLEXIBILITY

This is the capacity and flexibility to evolve mitigation plans which are an essential feature of dynamic resilience. For example, determining clear governance structures in advance of any cyber event so that the organisation understands who has the authority to determine a change in response plans during an ongoing cyberattack.

REGENERATIVE AND PREVENTATIVE CAPACITY

This is the process to support a transformative approach that enables adaption and innovation of the cyber risk management framework and includes an assessment of existing resources, systems, and capabilities to prevent future comparable attacks and enhance normal operational function. For example, an immediate goal during an event is to return to “normal operations” as swiftly and effectively as possible. However, lessons learned should be captured to evolve the response mechanisms and processes. A consistent review process should be established as part of dynamic resilience.

[10] To Survive or Thrive: How Crises Impact Company Value, Marsh, December, 2018

DIGITAL EVENTS REQUIRE DISTINCT PREPARATION PROCESSES

The energy sector has a strong safety record and history of preparing for operational risk events and natural catastrophes. For example, the power sector is generally well-versed and experienced in responding to physical exposures like extreme weather events (such as hurricanes, tornadoes, ice-storms) with established mechanisms, protocols, and mutual aid agreements to help systems come back online.

However, the sector’s experience with operational safety or responding to natural catastrophes may give it undue confidence in its ability to respond to digital events and disruptions. Operational safety experience does not equate to digital security. The processes, policies, and people necessary to respond to the characteristics of digital or cyber events, as compared to natural catastrophes, can be distinct. (See Exhibit 5.)

Exhibit 5: Characteristics of impacts of extreme weather events and digital events

Natural catastrophes	Digital event / cyberattacks
Localised impact on assets	Rapid expansion across assets in multiple sites and geographies and potential to become a systemic issue
One-time event with a forecastable start and end point (i.e., typically a few days)	Recurring event with no forecastable end-point (e.g., an advanced persistent threat attack in which the cybercriminal gains unauthorised access to a network and remains undetected for an extended period)
Threat proceeds with predictable patterns	Threat can cascade within and beyond the organisation with unpredictable patterns
Speed and velocity of threat can be predicted	Unpredictable speed and velocity of event
Threat does not alter or adapt in response to mitigation efforts	Threat can adapt in response to mitigation efforts (e.g., a data "wiper”)

Source: Marsh & McLennan Companies

GAMING EXERCISES TO BUILD DYNAMIC RESILIENCE

An essential component of dynamic resilience is preparing for response and recovery. Dynamic resilience recognises that if an attack occurs, an organisation’s ability to isolate the problem, and then mitigate and restore normal activities promptly, could define the future success of the business. A recent survey of the energy and power sector identified that respondents were relatively confident in their understanding of their cyber risk exposure, as well as mitigating and preventing such attacks, but had lesser confidence about their ability to recover from cyber incidents.[11]

The processes and mechanisms for response and recovery of digital energy infrastructure are less tested than responses to physical events. This is further complicated by many firms being reluctant to admit their digital and cyber incidents in case they become a more attractive target draw public or investor scrutiny. This makes the task of establishing and sharing best practice behaviour more challenging so an approach using hypothetical gaming exercises offers a potential solution to these sensitivities.

Cyber and digital disruption exercises, such as scenario planning and gaming workshops structured around risk exposures, are essential to identify specific vulnerabilities and better understand where the organisation needs to improve its overall cyber risk management framework. Most importantly, such exercises teach leaders how to manage through the attack

[11] Marsh-Microsoft Global Cyber Risk Perception Survey, 2019

and after the attack to remediate damage.[12] Overall, they help organisations develop muscle memory to defend against different types of scenarios.[13] However, one survey shows that just 46% of energy companies have conducted cyber risk management tabletop exercises or training for management in the past 12 to 24 months.

COUNTRY-LEVEL EXERCISES TO BUILD RESILIENCE ACROSS THE UTILITY SECTOR

Although tabletop exercises typically focus on preparations by an individual organisation, in the US, participants in the utility sector have collaborated in industry-wide exercises that simulate cyber and physical attacks that affected the reliable operation of the grid. For example, North American Electric Reliability Corporation (NERC) conducted its fourth biennial grid security and emergency response exercise (GridEx IV, November 15–16, 2017) with 6,500 individuals and 450 organisations participating across industry, law enforcement, government agencies, and state/provincial and local governments in the US, Canada, and Mexico. More recently, in November 2018, dozens of representatives from major US utilities and industry groups participated in a gaming exercise called Liberty Eclipse. The exercise was built around a scenario where many parts of the US grid had already been offline for a month, exhausting battery backups at power plants and substations.

Tabletop exercises are carefully planned to simulate actual cyberattacks with various stakeholders—C-suite executives, heads of business units, or both—responding with potential actions and reactions, as well as their assumptions and expectations behind those actions. A prepared moderator and team facilitate the exercise and often apply complicating factors such as misinformation, distractions, extreme weather events, or timing. Cyber experts and technicians are also in attendance to challenge assumptions or proposed actions.

Ideally, the exercise is a one-or two-day offsite to enhance the active engagement of responsible senior managers from different levels and areas of the business (including security specialists and top level executives). It is important to consider who needs to attend such exercises to ensure the necessary cross-functional expertise (technical, legal, customer relations, etc.) is provided with the opportunity to learn from the event and gain insights about each function's capabilities (or not) in the event of an digital incident.

Through the exercises, participants are asked to react to scenarios and consider business impacts and responses.[14] For instance:

[12] Is Your Company Ready for a Cyberattack? Paul Mee and James Cummings, Oliver Wyman, MIT Sloan Management Review, December 4, 2018

[13] Preparing for a Cyberattack, Paul Mee and James Cummings, Oliver Wyman, 2018

[14] Cyber Incident and Breach Response Planning: Is It Optional Any Longer? Marsh, November, 2018

- What is the financial impact of the loss of a specific business system, application, or database?
- How can we run the business if we lose a specific business system, application, or database, including corporate email and communication systems?
- What is the quickest way to bring affected business systems, applications, or databases back online, even if only in a limited capacity?
- What are the implications if externally facing business systems or web applications are no longer available to the business?
- If data security is breached and sensitive customer data is stolen, what would the company need to do?
- How would the organisation respond to misleading information about the event on social media?

APPLYING LESSONS TO BUILD DYNAMIC RESILIENCE

The analysis of lessons learned through scenario exercises is a crucial element in building dynamic resilience as these exercises typically uncover vulnerabilities or weaknesses in the organisation's baseline capabilities and cyber risk management framework that are often unrelated to IT networks or software. In particular, cyber gaming exercises can help identify opportunities to strengthen the following areas:

STRESS-TESTING THE RESILIENCE OF RECOVERY

Cyber exercises often identify vulnerabilities in three areas: internal communications, response governance, and external communications. Digital disruptions or cyberattacks can impact critical communications capabilities vital to the implementation of standard response protocols. A cyber response plan housed only on the corporate network may be of little use in a ransomware attack. Organisations need to consider the resilience of communication plans and if critical information is available in a non-digital format. For example, a major space weather event could damage electronic and communication infrastructure on an economy-wide basis. A malicious ransomware attack can limit access to company networks and laptops, and along with that, vital technical information, telephone numbers, and contact points. During the 2019 cyberattack on the aluminium maker Norsk Hydro, plants were able to continue production by relying on the knowledge of retired workers and paper manuals.[15]

Such exercises also help the organisation test the governance for decision-making during an event and whether there are clearly defined and pre-established roles and responsibilities at all levels of the organisation with authority to make necessary decisions. Responding to an event will be a shared responsibility of system operators, control engineers, information technology staff, and cybersecurity professionals, as well as business leaders from an array of functions such as government relations and customer services. Organisations must consider which executive will be the decision maker for critical decisions such as shutting down systems or determining when business systems can be restored. Will it be operational leaders such as the Chief Operating Officer, the Chief Information Officer, or the Chief Information Security Officer? And who has the authority in a given unit or geography?

[15] "When Cyberattack Hit Norsk Hydro, It Was Already Handling a Major Upheaval," Insurance Journal, April 9, 2019, https://www.insurancejournal.com

It is also important to consider the effectiveness of this governance structure under various scenarios. For example, if key actors are offsite, can remote action be easily taken? Are there redundancies built in to critical "call trees" if a key decision maker cannot be reached? How do weekends, holidays, or vacations impact the governance of responses? [16]

Organisations must also consider external communications and what information needs to be communicated to regulators, police, government officials, as well as other business stakeholders including insurers, and when to communicate this information.[17] In the US, the Department of Energy and the Federal Energy Regulatory Commission are both restructuring the rules for utilities to report grid cyberattacks to regulators and are broadening the definition of what constitutes a reportable incident.[18] The format and timeliness of communications to customers, staff, and the media are also essential. A key learning of the US's GridEx 2017 exercise was the need to focus on social media in external communication procedures and how to address misleading or false information on social media.

TESTING MECHANISMS FOR INTRA - AND INTER-SECTOR COORDINATION

Gaming exercises allow the organisation to ask: "Do the right people understand how coordination will occur, within the company and with other critical actors across the industry, and with local, regional, national, and possible international regulators and governments?"

A significant failure of the electricity system could trigger a series of cascading impacts, destabilising the wider economy and society. In such circumstances, recovering the power sector will be one of many co-dependent priorities and it is critical that there are pathways and mechanisms for cooperation and coordination within the sector and key stakeholders, such as local municipalities or governments, to prioritise actions. Organisations must consider how priorities for restoring energy services to critical infrastructure such as water utilities, hospitals, and data centers be set and agreed. It is also important to have cooperation and coordination at international levels given the cross-border characteristics of energy systems.

Due to the networked nature of many operations today, cultivating the right relationships is critical to building dynamic resilience. Coalitions with industry peers, regulators, industry associations, strategic partners, and law enforcement are critical elements of baseline capabilities and can help to establish predefined channels and mechanisms to improve situational awareness during an attack and facilitate agility and speed of response. For example, in the US, the Cyber Mutual Assistance program provides a pool of utility cybersecurity experts who volunteer to share their expertise with other utilities in the event of a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency.[19]

TEST PROTOCOLS AND MECHANISMS FOR EFFECTIVE RECOVERY

In the event of a cyberattack or a digital disruption, decisions taken in the response phase can have lasting impacts on the pace and effectiveness of recovery of the full system. In the scramble to get systems back on as fast as possible, decisions may be taken that expedite restart processes but increase vulnerability to further disruptions or attacks. For example, data integrity may also be compromised if systems are brought back online before proper defenses have been established to prevent further cyberattacks. The organisation also needs to consider if an initial cyberattack be a smoke screen to divert attention from another (perhaps even larger) attack. Gaming exercises provide an opportunity to consider the optimal pathways to recover the system while not creating future challenges.

Organisations can also use scenarios to consider and test assumptions about existing cyber insurance coverage and traditional property and liability insurance policies, which may not implicitly include or exclude cyber risks. Cyberattacks can be costly events and require significant resources to recover once the immediate crisis is over. In many instances, organisations go through a lengthy and costly forensic recovery effort requiring specialist expertise to recover data that has been corrupted, manipulated, or rendered inaccessible. For example, the cost of the cyberattack on Maersk is estimated at over US$300 million.[20]

Cyber insurance can play a foundational role in mitigating recovery costs. These can include: business interruption loss (e.g., loss of profit or increased costs of working during the period of downtime and any additional specified period); incident response costs (e.g., notification costs, call center costs, credit monitoring costs, and public relations costs); IT forensics; replacing damaged hardware; digital asset restoration; damage to persons or real property; and, cyber ransom and extortion costs.

Insurance should be viewed as an important component in strengthening a dynamic resilience framework. The process of renewing or purchasing cyber insurance coverage supports the development of baseline capabilities and the other elements of dynamic resilience as insurers can share aggregate lessons learned and recommend opportunities to resilience.

SECTOR NEEDS TO STRENGTHEN DIGITAL SKILL SETS

Preparation exercises may be particularly valuable in the energy sector where experience and expertise in working in a digital ecosystem may be lagging. Eight in 10 organiations in the energy sector, are not actively recruiting skills to support digital transformation, automation, and AI.[21] In general, the energy sector lacks sufficient skilled talent due to an aging workforce, workers who left the industry because of layoff fatigue, and younger potential employees whose value propositions are more in line with those of tech firms and startups. The advance in digitalisation means companies need to reskill and upskill existing employees as well as attract a new cadre of skills into their organisation to design, engineer, analyse, program, operate, and fix the software and equipment that are enabling the sector's digital transformation.

[16] Preparing for a Cyberattack, Paul Mee and James Cummings, Oliver Wyman, 2018

[17] Is Your Company Ready for a Cyberattack? Paul Mee and James Cummings, Oliver Wyman, MIT Sloan management Review, December 4, 2018

[18] https://www.eenews.net/stories/1060281821

[19] https://www.nerc.com

[20] The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired.com, August 8, 2018

[21] 2018 Spot Poll of 139 Global Energy Firms, Start Building Your Energy Workforce Of the Future, Today, Mercer, 2018

LOOKING FORWARD: NEW TOOLS TO STRENGTHEN RESILIENCE

The digitalisation of the energy industry will continue. As the industry relies more on interconnectivity, the potential for cyberattacks to cause severe disruption to operations, loss of data, and financial losses should remain a key concern for energy executives. In response, building and maintaining dynamic resilience must be seen as a continuous exercise. A regular cadence of exercises will develop an organisation's muscle memory to respond and help identify when and how overall digital resilience can be strengthened.

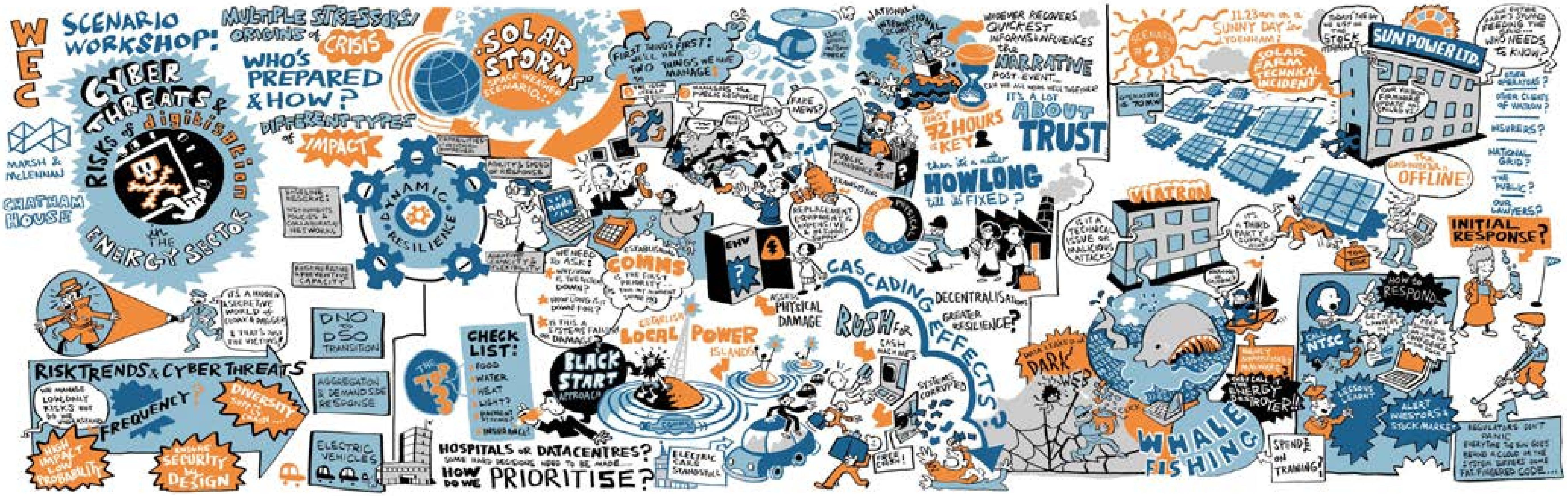
Since 2016, Marsh & McLennan and Swiss Re Corporate Solutions have been working with the World Energy Council to improve the resilience of the energy sector as part of a broad research programme. This has included a focus on strengthening digital and cyber resilience with the development of cyber scenarios and hypothetical gaming approaches that can be used by the Council's members.

The scenarios were recently tested at a pilot workshop organised with Chatham House. The learnings from this pilot exercise are captured in this report and summarised in Exhibit 6.

Going forward, the Council, Marsh & McLennan, and Swiss Re Corporate Solutions will continue to build the cyber resilience programme for roll-out across the global community of energy industry and policymakers. Our objective for the cyber resilience programme is to create a scalable platform that can be used within individual companies, by the Council's national member committees individually and regionally, and internationally where there can be a safe space to learn and develop best practice approaches. To support this Digital Energy Action Learning programme, a series of articles, webinars, and workshops will be developed that will be offered to the Council's community.

With the increasing sophistication of cybercriminals and the rising complexity of the digital energy sector, there are always new vulnerabilities to protect against. Engaging in the Council's research, accessing the evolving tools, and attending conferences and webinars, will allow the energy sector to continue to strengthen its digital resilience. We invite all interested parties to participate in this exciting and important area.

Exhibit 6: Cyber threat scenario workshop summary


WEC
SCENARIO WORKSHOP!
MARSH & McLENNAN
CHATHAM HOUSE
CYBER THREATS & RISKS of digitisation in THE ENERGY SECTOR
MULTIPLE STRESSORS/ ORIGINS of CRISIS
WHO'S PREPARED & HOW?
DIFFERENT TYPES of IMPACT
SOLAR STORM SPACE WEATHER SCENARIO...
DYNAMIC RESILIENCE
ABILITY & SPEED OF RESPONSE
IT'S A HIDDEN & SECRETIVE WORLD of CLOAK & DAGGER & THAT'S JUST THE VICTIMS!
RISK TRENDS & CYBER THREATS
FREQUENCY?
DIVERSITY
HIGH IMPACT LOW PROBABILITY
SECURITY by DESIGN
DNO to DSO TRANSITION
AGGREGATION & DEMAND SIDE RESPONSE
ELECTRIC VEHICLES
CHECK LIST:
FOOD
WATER
HEAT
LIGHT?
INSURANCE?
HOSPITALS or DATACENTRES?
HOW DO WE PRIORITISE?
FIRST THINGS FIRST: WE'LL HAVE TWO THINGS WE HAVE MANAGE!
MANAGING the PUBLIC RESPONSE
FAKE NEWS?
WE NEED to ASK:
HOW LONG IS IT DOWN FOR?
IS THIS A SYSTEMIC FAILURE or DAMAGE?
COMMS IS THE FIRST PRIORITY...
BLACK START APPROACH
ESTABLISH LOCAL POWER ISLANDS
EHV
REPLACEMENT EQUIPMENT IS EXPENSIVE
PHYSICAL DAMAGE
CASCADING EFFECTS?
RUSH for CASH MACHINES
SYSTEMS CORRUPTED
FREE CASH!
DECENTRALISATION GREATER RESILIENCE?
ELECTRIC CARS STRANDED
WHOEVER RECOVERS QUICKEST INFORMS & INFLUENCES the NARRATIVE POST-EVENT...
IT'S A LOT ABOUT TRUST
FIRST 72 HOURS is KEY
then it's a matter HOW LONG till it's FIXED?
IS IT A TECHNICAL ISSUE or MALICIOUS ATTACK?
SCENARIO 2
11.23am on a SUNNY DAY in ...
SOLAR FARM TECHNICAL INCIDENT
SUN POWER LTD.
WHO NEEDS to KNOW?
OTHER OPERATORS?
OTHER CLIENTS OF VIATRON?
INSURERS?
NATIONAL GRID?
THE PUBLIC?
OUR LAWYERS?
OFFLINE!
VIATRON
IT'S A THIRD PARTY SUPPLIER
INITIAL RESPONSE?
HOW to RESPOND
NTSC
LESSONS LEARNT
ALERT INVESTORS & STOCK MARKET
DARK WEB
WHALE FISHING
ENERGY DESTROYER
SPEND on TRAINING?
REGULATORS DON'T PANIC

Source: World Energy Council, Marsh & McLennan, Chatham House, 2019. Workshop Artwork by Joshua Knowles, 2019, www.joshknowles.co.uk

ABOUT THIS DYNAMIC RESILIENCE INSIGHTS BRIEF

This Dynamic Resilience Insights Brief on Digital Resilience is part of a broader programme by the World Energy Council, in partnership with Marsh & McLennan and Swiss Re Corporate Solutions, to improve resiliency of the whole energy system as it evolves with the Grand Transition. Achieving resiliency of whole energy systems involves anticipating systemic risks and developing the capacity of the whole system to absorb (withstand and endure), recover (promptly and creatively) and adapt to new and faster changing conditions. The Dynamic Resilience programme facilitates strategic knowledge sharing for emerging and systems risks and new types of energy shock between the Council's members and the other energy stakeholders and policy shapers.

This report was prepared and developed with Marsh & McLennan Insights of Marsh and McLennan Companies.

ABOUT MARSH & MCLENNAN INSIGHTS

Marsh & McLennan Insights uses the unique expertise of our firm and its networks to identify breakthrough perspectives and solutions to society's most complex challenges. Marsh & McLennan Companies is the world's leading professional services firm in risk, strategy, and people. Through its market-leading firms—Marsh, Guy Carpenter, Mercer, and Oliver Wyman—Marsh & McLennan's more than 75,000 colleagues provide analysis, advice, and transactional capabilities to clients in over 130 countries.

PROJECT TEAM

Lucy Nottingham (Director, Marsh & McLennan Insights), Martin Young (Director, World Energy Council)

MARSH & MCLENNAN COMPANY PRINCIPAL CONTRIBUTORS

Rob Bailey, (Director, Marsh & McLennan Insights), Leslie Chacko, (Director, Marsh & McLennan Insights), James Crask, (Senior Vice President, Marsh Risk Consulting), Andrew Herring, (Managing Director, Energy & Power Practice, Marsh), Matthew McCabe, (Senior Vice President, Marsh), Paul Mee, (Partner, Oliver Wyman), Sandro Melis, (Partner, Oliver Wyman), Kevin Richards, (Global Head of Cyber Risk Consulting, Marsh Risk Consulting), Sarah Stephens, (FINPRO Cyber, Media & Technology Practice Leader, Marsh JLT Specialty), James Sutherland, (Director, MMC Advantage, Marsh & McLennan Companies), Jaclyn Yeo (Manager, Marsh & McLennan Insights), Alex Wittenberg (Executive Director, Marsh & McLennan Insights)

SWISS RE CORPORATE SOLUTIONS CONTRIBUTORS

Juerg Trueb, (Managing Director and Head Environmental & Commodity Markets, Swiss Re Corporate Solutions Ltd)

WORLD ENERGY COUNCIL CONTRIBUTORS

Jan Bartos (Consultant), Cliodhna O'Flaherty-Mouscadet (Senior Manager), Joshua Oyinlola (Coordinator), Jorge Romeo (Manager), Alexandre Tourbah (Intern), Natalie Vintners (Associate Director), Maria Vinograd (Manager), Angela Wilkinson (Senior Director)