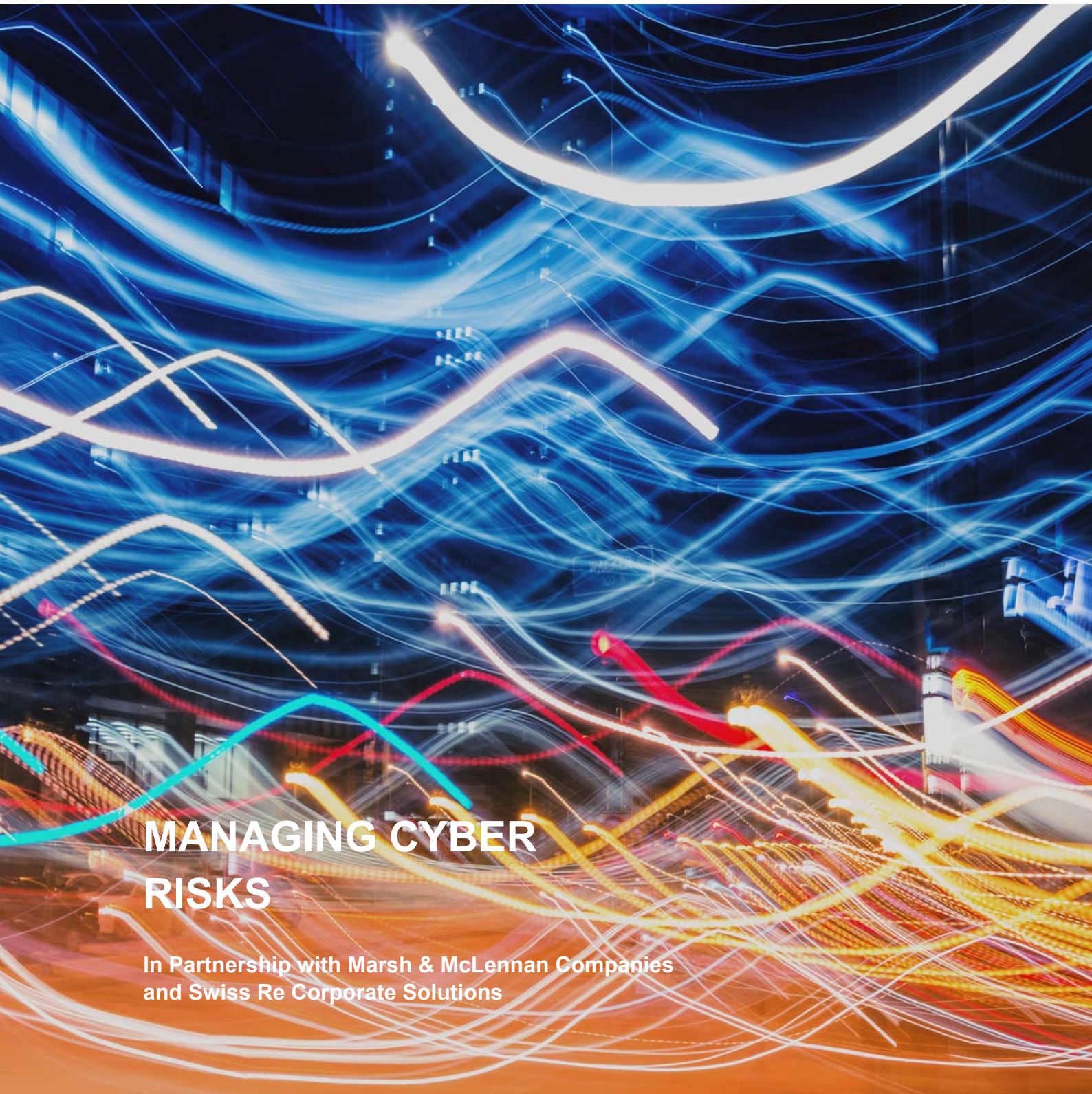
WORLD ENERGY COUNCIL

# World Energy Perspectives

The road to resilience | 2016



## MANAGING CYBER RISKS

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

## ABOUT THE 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.

Formed in 1923, the Council is the UN-accredited global energy body, representing the entire energy spectrum, with over 3,000 member organisations in over 90 countries, drawn from governments, private and state corporations, academia, NGOs and energy stakeholders. We inform global, regional and national energy strategies by hosting high-level events including the World Energy Congress and publishing authoritative studies, and work through our extensive member network to facilitate the world's energy policy dialogue.

Further details at www.worldenergy.org and @WECouncil

## ABOUT THE ROAD TO RESILIENCE - MANAGING CYBER RISKS

The road to resilience – managing cyber risks is the third risk dimension investigated as part of the Financing Resilient Energy Infrastructure initiative. This report, prepared in partnership with Marsh & McLennan Companies and Swiss Re Corporate Solutions, investigates how cyber risks can best be managed, taking into account the changing nature of the energy industry and energy infrastructure. Drawing on insights from a network of energy industry experts, the report assesses the ways in which vulnerabilities in current and new energy infrastructures are changing. The report recommends actions that energy decision makers and stakeholders can take – individually and collaboratively – to improve the sector's response to rising cyber threats, as part of a wider move towards resilience.

Prepared in partnership with Marsh & McLennan Companies and Swiss Re Corporate Solutions

# CYBER-ATTACKS IN THE ENERGY SECTOR CAN IMPACT THE WIDER ECONOMY.

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

**Greater resilience to cyber risk is critical to current and future energy security. The internet and networked technologies have changed many aspects of the energy sector. Increased digitisation, through devices such as smart meters, continues to create efficiencies and offers operators the opportunity to improve grid management, pipeline management and exploration and production. At the same time, with these benefits come associated increased vulnerabilities, in particular due to the automation of Industrial Control Systems (ICS). Attacks on ICSs could lead to loss of control of key equipment which could have damaging consequences in the physical world. This could include machinery breakdown, fire, explosion or injuries, with significant impacts on the operations of energy assets, local communities and the economy.**

This report investigates how cyber risks can best be managed, taking into account the changing nature of the energy industry and energy infrastructure. Drawing on insights from a network of energy industry experts, the report assesses the ways in which vulnerabilities in current and new energy infrastructures are changing. The report recommends actions that energy decision makers and stakeholders can take – individually and collaboratively – to improve the sector's response to rising cyber threats, as part of a wider move toward greater resilience.

## KEY FINDINGS

1. **CYBER THREATS ARE AMONG THE TOP CONCERNS** for energy leaders, especially in countries with high infrastructure maturity, particularly North America and Europe. In these regions, energy leaders are increasingly recognising the importance of viewing cyber-attacks as a core threat to business continuity, and the need to create an organisation-wide cyber awareness culture that extends beyond traditional IT departments.

2. **INCREASING INTERCONNECTION AND DIGITISATION** of the energy sector (including smart grids, smart devices and the growing internet of things) and its critical role in the functioning of a modern economy make the energy sector vulnerable to cyber-attacks aimed at disrupting operations. Although digitisation increases operational efficiency in the industry, growing interconnection also raises the complexity of cyber risk management.

3. **CYBER RISK PRESENTS A UNIQUE CONCERN** in the energy sector because an attack on energy infrastructure has the potential to cross from the cyber realm to the physical world – a cyber-attack could cause, for instance, a massive operational failure of an energy asset. Large centralised infrastructures are especially at risk due to the potential 'domino effect' damage that an attack on a nuclear, coal, or oil plant could cause.

4. **TECHNOLOGY VENDORS CAN PLAY A CRITICAL ROLE** in furthering, or hindering, the resilience of energy infrastructures. These firms must ensure that they deliver technologies that have security standards built into their products. Without doing so, ICS and supervisory control and data acquisition (SCADA) controls can compound cyber risks, and increase the vulnerability of energy operations to attack.

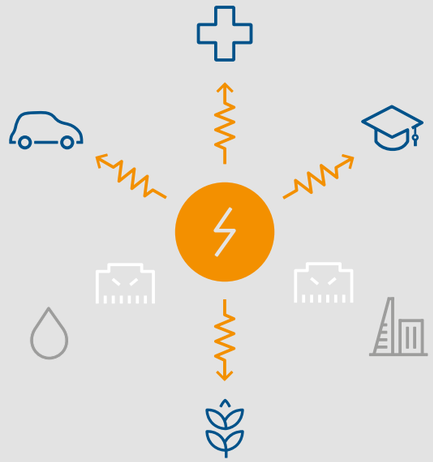
5. **COMPANIES ARE INCREASINGLY RECOGNISING CYBER** as a core risk, there is insufficient information sharing among industry members and across sectors on cyber experiences. Improved information sharing within the sector and between public and private stakeholders would enable greater understanding of the impact of cyber risks to energy companies and to the sector as a whole. In addition, employees' awareness of cyber vulnerabilities must be included as part of an effective cybersecurity strategy. Human error is very often a key factor in the success of cyber-attacks, due to insufficient awareness of cyber risks among staff at all levels of the organisation.

6. **CYBER INSURANCE IS ONE MECHANISM** to help offset potential financial losses from a cyber-attack. However, the insurance industry must continue to develop instruments to address the potentially catastrophic losses and the complexity of cyber risk. As an emerging and evolving risk, there is limited historical data related to cyber; this restricts the maturity of the cyber insurance market. Nevertheless, the process of applying for cyber insurance in itself is often beneficial for companies, as it forces them to assess their cyber practices.

# THE ROAD TO RESILIENCE: MANAGING CYBER RISKS

WORLD ENERGY COUNCIL

## ENERGY INFRASTRUCTURE: THE HEART OF ALL MODERN ECONOMIES

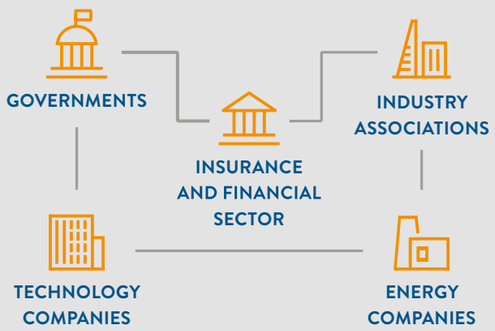


Cyber risks are growing in terms of both their sophistication and the frequency of attacks. The economic and physical consequences of cyber-attacks on energy infrastructure could be severe, making it an attractive target.

## RECOMMENDATIONS

All stakeholders must work together across 4 areas to tackle cyber risks:

- Technical and human factors
- Information sharing on cyber risks
- Risk assessment and quantification
- Developing standards and best practices




## INCIDENTS CASE STUDIES

### 1 USA AND CANADA, 2013–2015
**POWER GENERATION**
**Human error // hacking**

This attack on a company that operates over 50 power plants in the US and Canada began through information stolen from a contractor. Hackers were able to steal critical power plant designs and system passwords.

### 2 USA, 2003
**NUCLEAR POWER PLANT**
**Malware**

'Slammer' was the fastest computer worm in history. In 2003 it attacked the private network at an idle nuclear power plant in Ohio, disabling a safety monitoring system for 5 hours. Five other utilities were also affected.

### 3 USA, 2012
**POWER GENERATION**
**Human error // virus**

A US power utility's ICS was infected with the Mariposa virus when a 3rd-party technician used an infected USB drive to upload software to the systems. The virus resulted in downtime for the systems and delayed plant restart by approximately 3 weeks.

### 4 USA, 2013
**NON-ENERGY INFRASTRUCTURE**
**Malware**

The small Bowman Avenue Dam, near New York City, is used for flood control rather than power generation. Hackers gained partial access to the dam's systems using standard malware, highlighting the vulnerability of all infrastructures.

### 5 UKRAINE, 2015
**POWER GRID**
**Hacking // human error**

This well-planned hack on 3 power-distribution companies caused outages to 80,000 energy customers. It is the first known hack to cause a power outage. The hack began with a spear-phishing campaign targeted at the companies' IT staff.

### 6 SAUDI ARABIA, 2012
**OIL COMPANY**
**Virus**

The Shamoon virus infected 30,000 computers belonging to Saudi Aramco, the world's largest oil and gas producer. Some systems were offline for 10 days, and 85% of the company's hardware was destroyed. The entire national economy was affected.

### 7 NETHERLANDS, 2012
**TELECOMMUNICATIONS**
**Hacking**

A 17-year-old was arrested for breaching hundreds of servers. The servers were maintained by a telecommunications company providing smart-meter services to utilities.

### 8 GERMANY, 2014
**MANUFACTURING**
**Hacking**

Hackers attacked the business network of a German steel mill, and from there its production network, causing 'massive' damage to their industrial equipment. It was the second recorded cyber-attack to affect physical infrastructure.

### 9 ISRAEL, 2016
**PUBLIC SECTOR; POWER GRID**
**Malware // human error**

An employee of the Electricity Authority fell for a phishing attack, which infected a number of computers on the network with malware. The power grid was not affected, but it took two days for the Authority to resume normal operation.

### 10 SOUTH KOREA, 2015
**NUCLEAR POWER PLANT**
**Hacking**

Korea Hydro and Nuclear Power Co. suffered a series of attacks aimed at causing nuclear reactors to malfunction. The attacks only succeeded in leaking non-classified documents.

### 11 AUSTRALIA, 2015
**PUBLIC SECTOR**
**Hacking // virus**

Hackers attacked the Maitland office of the Department of Resources and Energy in New South Wales. The hackers may have been interested in the department's current projects, or may have viewed it as a weak link to access more highly classified government information.

The sophistication and number of cyber-attacks is growing.

The first real incidents in the energy system have been experienced.

By 2018 the oil and gas industries could be spending US$1.87 billion each year on cyber security.

## IMPLICATIONS FOR THE ENERGY SECTOR

As the energy sector seeks to improve its efficiency and reliability, infrastructure operators must be aware that the increased use of the internet of things also increases vulnerability to cyber-attacks across the energy value chain.

Cyber risk must not be considered purely as an IT risk but it should be addressed as an enterprise-wide concern and as a key operational risk that requires effective and comprehensive risk management, including governance and oversight from the board of directors and executive team.

The energy sector must take a systemic approach and assess cyber risks across the entire energy supply chain, to improve the protection of energy systems and limit any possible domino effects that might be caused by a failure in one area of the value chain. Nevertheless, measures that require supply chain compliance or cross-border cooperation are more difficult to implement, and require increased cooperation across sectors.

Companies should implement measures to prevent, detect and respond to cyber threats. This includes both technical measures of resilience (security measures for software and hardware, measures governing physical structures, such as limiting access to data centres, and clear instructions for using external hard drives), and human resilience measures built on developing a robust cyber awareness culture within and beyond organisations.

Working across sectors and collaborating with governmental and private sector institutions can help companies gain a better understanding of the nature of cyber risk impacts. International cooperation must be enhanced to strengthen the cyber security and resilience of energy systems. Disseminating information about incidents, sharing best practices and introducing international cyber security standards are key elements for addressing the challenge.

If the energy and utility industry implements risk protection and resilience measures, the financial and insurance communities will be able to provide coverage for damages at achievable prices. Cyber-attacks in the energy sector have an impact not only on the sector itself, but on the wider economy and the whole fabric of a state. Further, as informatics technology and cyber threat vectors constantly change, partly in response to defences, insurers will be faced with the challenge of accurately assessing the impact of cyber-attacks; historical data might not be sufficient. Better information from the energy industry will help the insurance industry improve its coverage of energy assets. Still, energy companies also need to identify more clearly where insurance is most needed to fill the protection gap, and they must work with underwriters to further develop cyber insurance products.

## RECOMMENDATIONS

All key stakeholders must play an active role in managing cyber risks:

- **Insurance and financial sector:** must adapt coverage to meet the ongoing evolution of cyber risk. The sector must work with the energy industry to improve awareness of cyber insurance products, further develop the cyber insurance market, and, allied with this, support the energy industry in determining and collating critical cyber risk data. The sector must stay informed of the constantly evolving technological developments, as these will inform the insured risks. They must monitor cyber risks covered within existing insurance products, and adapt where necessary, for example through pricing or limiting, and focus on managing newly arising and changing accumulation risks. Finally, the insurance and financial sector must respond to evolving cyber regulation.

- **Energy companies:** must view cyber risk as a core business risk, effectively assess and understand company-specific cyber risks and build strong technical and human resilience strategies. Companies must work to increase awareness among other energy stakeholders of the impact of cyber-attacks; this will ensure that the broader energy community are included in resilience measures.

- **Governments:** must support strong responses from companies to cyber risks by stimulating the introduction of standards or imposing dedicated regulations. However, regulatory and reporting requirements should not become overly complex for this dynamic risk. Governments must support information sharing across countries, sectors and within the industry, and they must improve international cooperation on cyber security frameworks.

- **Technology companies serving the energy sector:** must embed security features and considerations when developing technologies, and work with the energy sector to use the latest technologies to monitor the nature of cyber-attacks.

- **Industry associations:** must support and stimulate information sharing and the adoption of best practices, conduct peer evaluations, and help companies and the sector develop a robust and active cyber-aware culture.

**80% OF OIL AND GAS COMPANIES SAW AN INCREASE IN THE NUMBER OF SUCCESSFUL CYBER-ATTACKS IN 2015.**

# INTRODUCTION

On 15 August 2012, Saudi Aramco, the state-owned group that runs all of Saudi Arabia's oil production, suffered a virus attack that damaged approximately 30,000 computers by malware infestation and destroyed 85% of the hardware on the company's devices. The virus, called 'Shamoon', did not just target Saudi Aramco as an entity; it attacked the country's entire economy.

On 23 December 2015, hackers entered the computer and SCADA systems of the Ukrainian electricity distribution company Kyivoblenergo and disconnected seven 110 kV and twenty three 35 kV substations, causing a 3-hour outage for around 80,000 customers. This attack was the first publicly acknowledged cyber event impacting a country's power supply.

Many cyber incidents target sensitive and financially lucrative data, such as credit card information, banking data, medical records or business trade secrets. In 2015 alone, 736 million data files worldwide were potentially viewed or stolen. However, other cyber-related threats exist in today's risk landscape and the effective functioning of critical infrastructures is increasingly at risk. Over 80% of oil and gas companies saw an increase in the number of successful cyber-attacks over the past year.[1]

The energy sector is of particular concern where an attack on an operating system could cause infrastructure to shut down, triggering economic or financial disruptions or even loss of life and massive environmental damage. The potential for physical damage makes this industry a prime target for cybercriminals, state-sanctioned cyber-attacks, terrorists, hacktivists and others looking to make a statement. For example, what would have happened if the attack on Saudi Aramco had caused a fire or explosion of the pipelines, refinery and/or storage facilities? What environmental damage would have arisen from an oil leak at the facilities? And what potential knock-on effects would emerge if one of the world's biggest oil producers were unable to provide a stable supply to the global economy?[2]

In a survey of critical infrastructure organisations in the United States (US), the United Kingdom (UK), France, and Germany, 48% of respondents expressed that it would be likely for a cyber-attack to take down critical infrastructure with the potential loss of life.[3] As one energy executive interviewed in the preparation of this report noted, "Energy companies must get used to the fact that cyber is now same kind of risk to a large infrastructure as a flood or a fire." In addition, the frequency, sophistication and costs of data breaches are increasing. For example, the US Department of Homeland Security Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) responded to 295 cyber

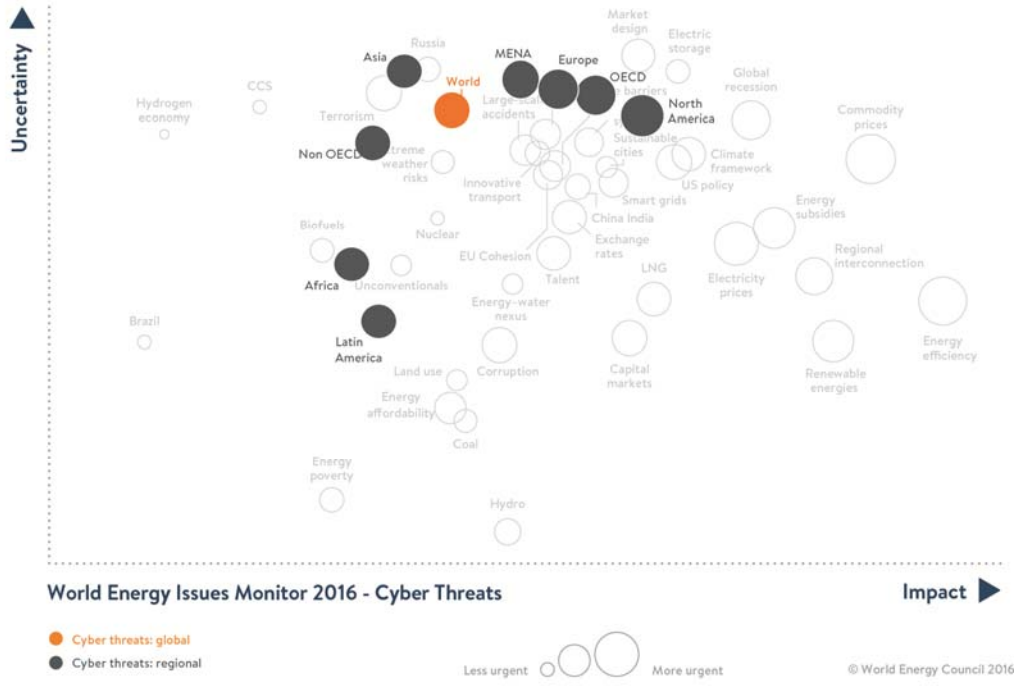
[1] Herring A, 2016: How Energy Companies Can Manage the Growing Threat of Cyber-Attack, 24 June 2016 (Marsh)
[2] Swiss Re, 2014: Gearing up for Cyber Risk
[3] The Aspen Institute and Intel Security, 2015: Critical Infrastructure Readiness Report: Holding the Line Against Cyber threats

incidents within the energy sector in 2015, a 20% increase compared to 2014. The energy sector accounted for 16% of the attacks, behind only critical manufacturing, at 33%. Another multi-country study found that the average annualised cost of cybercrime in the financial services and utilities and energy sectors is substantially higher than the cybercrime costs of organisations in healthcare, automotive and agriculture, with the average cybercrime cost in the utilities and energy sector at US$12.8m.[4]

In response to the rising threat, the investments required to protect against cyber risks are also increasing for the industry. By 2018 oil and gas companies globally could face costs of up to US$1.87bn in cyber security spending in an effort to protect themselves against cyber risks. In Europe alone, consulting and testing services associated with cybersecurity at utilities are expected to be €412m (US$564m) a year by 2016.[5]

The findings of the World Energy Issues Monitor, which began tracking cyber risks in 2014, show that the focus on cyber threats by energy leaders varies around the globe, but the concern over the potential impact and uncertainty of cyber threats has increased, especially in Europe and Northern America. (see Figure 1: Cyber threats a rising concern for global energy executives).

## FIGURE 1: CYBER THREATS A RISING CONCERN FOR GLOBAL ENERGY EXECUTIVES




Source: World Energy Council, 2016: World Energy Issues Monitor

[4] Ponemon Institute LLC, 2015: 2015 Cost of Cyber Crime Study: Global
[5] Bloomberg, 2014: Hackers find open back door to power grid with renewables

A better understanding of risks and the components of resilience is needed to increase collaboration among stakeholders to improve information and, where possible, data sharing. To help advance the understanding of such emerging and dynamic risks as cyber, the World Energy Council, in partnership with Marsh & McLennan Companies and Swiss Re Corporate Solutions, and with the support of a network of global experts from close to 40 countries, has developed a series of reports about Financing Resilient Energy Infrastructure. The reports focus on identifying and characterising the nature, frequency and severity of critical emerging risks and key recommendations to increase energy infrastructure resilience.

While there is no single definition of resilience for energy infrastructure, literature review reveals that resilience implies a functioning and stable system that ensures continuity. Energy infrastructure needs to be robust and recover operations swiftly if an event occurs to minimise service interruptions. They need to be able to withstand extraordinary events, secure the safety of equipment and people and ensure continued and reliable energy production. Establishing increased resilience requires improved risk assessment and modelling, better planning and design, and improved communication and collaboration.

As the global energy architecture evolves and expands to meet growing energy demands and the challenges of decarbonisation, policymakers and the energy sector need to increase and embed cyber resilience into energy assets. The nature and changing risk profile of the cyber threat – from economic espionage to disruption of production – demands a cross-industry risk-based approach from businesses and governments around the world.[6] Energy companies must treat cyber risks as permanent and persistent risks to their entire enterprise, and develop an organisation-wide cyber strategy to ensure effective risk management.

[6] Marsh, 2014: Advanced cyber-attacks on global energy facilities

“ENERGY COMPANIES MUST GET USED TO THE FACT THAT CYBER IS NOW THE SAME KIND OF RISK TO A LARGE INFRASTRUCTURE AS A FLOOD OR A FIRE.”

# DEFINING CYBER RISKS

Cyber risk is defined as any risk that emanate from the use of electronic data and its transmission, including technology tools such as the Internet and telecommunications networks. The risk also includes physical damage that can be caused by cyber-attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – whether it is related to individuals, companies, or governments. Cyber risks may emanate from a number of sources, often unforeseen, and the impacts can vary and may affect a business in a number of different ways. Attacks on critical infrastructure, such as industrial control systems, may be particularly severe and could have far-reaching consequences.

The risks and impacts can be due to human or system error but also to cybercrime that is often driven by traditional criminal motives, such as theft, robbery or sabotage, which can be executed without any need for physical proximity. As such, cybercriminals may be internal or external to an organisation, and their motives and drivers are varied and evolving. Attacks have stemmed from sabotage and lone hackers, from the use of malware, through to sophisticated networks or state sponsored attacks.[7]

Cyber risks include non-physical and physical damage from a cyber-attack. Non-physical damage includes:

- data corruption – which leads to an interruption of operations,
- theft of intellectual property – which might be sold to competitors,
- extortion or the threat of extortion,
- theft of private/financial data – which is a breach of privacy. Data theft can target customer information, such as credit cards and payment information; employee information, business partner information, but also business propriety information, such as company financial projections, forecasts, business strategy and geoscience data.

Physical damage consists of the infection of software – which can lead to manipulation of controls leading to breakdown of critical machinery and supply disruptions, especially in the energy industry. Cyber-attacks can impact assets and information resources, affecting the integrity and availability of operational technology (e.g., building and physical plant controls, manufacturing systems, SCADA systems, warehouse systems) and data.

The potential for cyber-attacks is increasing across all sectors of the economy and in all countries. Network technologies and systems are becoming increasingly modernised, automated, and interconnected. While these advancements enhance the systems' reliability,

[7] CRO Forum, 2014: Cyber resilience – The cyber risk challenge and the role of insurance

productivity, and efficiency, they also increase their exposure to cyber-attacks. As the internet of things develops within and across industries, the risk of cyber-attacks will grow.

Compounding the threat of cyber-attacks is the fact that cyber-attackers are adopting increasingly sophisticated methods. Cyber risks are dynamic threats that are constantly evolving; it is a game played against an adversary in which cyber past does not predict cyber future. As organisations' defences evolve, attackers adapt and innovate.[8] Of further concern, the most serious breaches remain undetected for considerable amounts of time. For example, UK government estimates indicate that on average, 200 days elapse between a security incident occurring and its detection, which means the attackers can roam undetected in breached environments during that period.[9]

[8] Marsh, 2015: Benchmarking Trends: Cyber-Attacks Drive Insurance Purchases For New and Existing Buyers
[9] CRO Forum, 2014: Cyber resilience – The cyber risk challenge and the role of insurance

# THE ENERGY SECTOR'S INCREASING EXPOSURE TO CYBER RISKS

The sector has been quick to take advantage of new internet-connected systems and digital technologies to reduce costs, improve efficiency, and streamline operations. The transformation of the energy sectors includes digitisation, evolving business models, distributed generation, and an increase in information and communication between utilities and customers around their energy consumption. In this context, three factors raise the stakes of cyber risks in the energy sector. Firstly, the ongoing digitisation of the energy sector is increasing its cyber vulnerability; secondly, the continuous evolution and sophistication of cyber-attacks present a highly dynamic threat; and thirdly, the sector's fundamental role in a functioning of economy and society and the potential cross-over between a cyber-attack and a physical event.

Cyber threats to the energy sector are not new - energy companies have long faced the risk of internal recklessness or sabotage. In the past the energy sector was able to leverage the protection offered by standalone and closed ICS as the primary barrier to the cybersecurity threat.[10]

As energy facilities worldwide age, upgrades and expansion projects include the adoption of integrated ICS and SCADA systems, many of which were designed on principles of openness and interoperability. The new systems have integrated control systems with other IT networks, and greater use of internet and IT networks. These enhancements provide business insight, remote access, and interoperability between systems (see Box 1: The digitisation of the energy industry). However, many ICS were developed and implemented at a time when cybersecurity was not necessarily a core concern and may not have the necessary levels of security for the new world of cyber-attacks.

The rising threats, sources, and impacts of cyber-attacks are common to many economic sectors, but the energy industry has specific and growing challenges across the extensive energy value chain from exploration to electricity distribution (see Table 1: Impact of cyber risks in the energy sector). Of particular concern in the energy sector is the potential for a cyber threat to cross over into physical damage to energy assets or the surrounding environments. Some subsectors of the energy industry may be targeted more than others. In 2014, for example, pipeline transportation had by far the highest number of incidents, followed by support activities for mining, oil and gas extraction.[11] Furthermore, these rates of cyber-attacks on the energy subsectors stand out compared to other industries.

Computer viruses such as Shamoon have drawn the energy sector's attention to the potential disruption that could be caused by a malicious piece of software, leading to a high level of concern across the industry.

[10] Marsh, 2014: Advanced cyber-attacks on global energy facilities
[11] Verizon, 2015: Data Breach Investigations Report

## TABLE 1: IMPACTS OF CYBER RISKS IN THE ENERGY SECTOR

| Impacts | Examples/Illustrations |
|---|---|
| **Market disruption** | Hacking into company data on reserves could impact derivatives and future market for oil and gas, and may cause industry-wide problems.<br><br>Accessing company information on coal reserves could include information related to commodity pricing. |
| **Physical infrastructure damage** | Attacks to dams and levees could result in massive property damage and compromise water supply.<br><br>Gaining control of a wind turbine could change the wind vane speed, damaging the equipment. |
| **National security** | Attacks on systems of national interest and critical infrastructure could have significant impacts on a country's economy, international competitiveness, public safety, or national defence and security.[12] |
| **Human harm** | An attack on nuclear plant equipment could lead to a core meltdown and dispersal of radioactivity.<br><br>An infiltration of the electric grid that results in black-outs can cut off access to running water, refrigeration or other services dependent on electricity. |
| **Network effects** | Breaching a control system at a generating facility could serve as an access point for another facility that has a larger impact, taking large portions of the grid offline.[13]<br><br>An attack could impact operations of solar panels and cut energy to a given area |
| **Financial loss, liabilities** | Attacks can lead to financial losses including the cost to replace broken equipment and upgrade systems affected by an attack, regulatory fines, loss of business opportunity, and loss of intellectual capital as well as – in a secondary stage – liability of power producers towards manufactures in case of continued business interruption and delays in manufacturing. |

[12] Hogan Lovells, 2016: Cybersecurity: A growing threat to the energy sector – An Australian perspective
[13] Wind power engineering and development, 2015: Cyber security and wind-farm penetrations

## BOX 1: THE DIGITISATION OF THE ENERGY INDUSTRY

Electric utilities increasingly depend on automated controls to run their grids, which are managed through interconnected network systems. Oil and gas companies depend on data networks to manage facilities and interpret operating conditions. Transmission companies rely on data networks to manage meters and to analyse their customers' needs. Control rooms, substations and devices used to manage oil and gas plants, refineries and pipelines are now all digital, utilising video-enabled telepresence and high-speed data links. Upstream, digital technologies are used for reservoir modelling, drilling resource dispatching, computer-aided hydraulic fracturing, production optimisation, reliability and preventive maintenance, and supply chain planning analytics.

Downstream, the shift to digital is being realised through supply-demand matching smart grids and new approaches to networking operational systems. Applications of digital technologies further downstream include trading activities and marketing and business insights.

This digitisation increasingly opens the sector to more potential points for cyber exposures and creates a higher volume of data that could be subject to data breaches or theft. The amount of data associated with the shift to digital is huge. For example, a large offshore field could deliver more than 0.75 terabytes of data each week, while a large refinery will produce 1 terabyte of raw data per day. [14]

The changing energy architecture, including the expansion of decentralised renewable generation assets and the smart grids to improve the management of electricity, create an increased number of entry points for cyber intruders.[15] The introduction of 'smart' solutions will require cybersecurity and power system communication systems to be dealt with simultaneously. These elements together are essential for proper electricity transmission, where the information infrastructure is as critical as the physical transmission infrastructure.[16]

For example, an attack on the power grid in Ukraine became the first publicly acknowledged cyber event which impacted the power supply of a country, when attackers remotely manipulated the utility's SCADA system (see Box 2: Ukraine power grid attack). Other potential targets include offshore drilling rigs, power generation plants, and pipelines exposed by direct connectivity to the internet and enterprise IT networks.

[14] Journal of Petroleum Technology, 2012: Data Mining Applications in the Oil and Gas Industry
[15] International Energy Agency (IEA), 2015: How to Guide for Smart Grids in Distribution Networks
[16] EU Agency for Network and Information Security, 2014: Smart grid security certification in Europe

## BOX 2: UKRAINE POWER GRID ATTACK

On 23 December 2015, hackers entered the computer and SCADA systems of the Ukrainian Kyivoblenergo, a regional electricity distribution company, and disconnected seven 110 kV and twenty three 35 kV substations, creating an outage for around 80,000 customers for three hours. Later, it became clear that attacks were attempted at three other distribution companies in parallel, raising the total outage, if successful, to 225,000 customers across the country.[17]

Following the attack, Ukrainian investigators, the US government, and international security experts conducted an analysis to ascertain the root cause of the outage. The investigation uncovered the sophistication in conducting a multisite and multistage attack, both in terms of advanced planning and technical capabilities. While the exact timeline of the attack coordination is unclear, investigators found evidence that hackers had completed long reconnaissance missions into the company's network to familiarise themselves with the environment beforehand. According to Electricity Information Sharing and Analysis Center (E-ISAC) analysis, the attackers used a variety of techniques including spear phishing emails, possibly variants of the BlackEnergy 3 malware, so-called 'KillDisk' malware, and embedding malware in Microsoft Office documents to gain access to the IT networks of the distribution companies. The attackers also demonstrated capabilities in operating the industrial control system through remote admin tools. After gaining access to the systems, the hackers went on to inflict further damage and paralyse the distributors by rendering field devices at substations inoperable and flooding the call centre with fake calls to prevent customers from reporting the outage.[18]

The attack exploited security lapses in the companies' corporate IT and SCADA systems as well as inadequate human factors management around cyber risk. Further vulnerability may have been created by having critical computers connected to the internet rather than running on a separate internal network. At the time of the attack, the distributors' SCADA systems, like those of many other utilities, were not designed with cybersecurity as a priority in mind; improved scanning for malicious signatures could have helped detect the attack. The Ukraine case study also demonstrates the importance of employee cybersecurity training, as the point of entry was a simple phishing scam.[19]

The risk of cyber-attacks is accentuated for new energy projects, which typically have greater levels of complexity and higher value concentration. Security and innovation need to be developed hand-in-hand and planned for from idea inception to product rollout and beyond.

Energy companies are witnessing significantly more intelligent and complex attacks that seek to take charge of ICS in order to inflict damage to property and operations. A survey of over 150 US-based IT professionals in the energy, utilities, and oil and gas industries that

[17] E-ISAC, 2016: Analysis of the Cyber Attack on the Ukrainian Power Grid
[18] Reuters, 2016: Hackers may have wider access to Ukrainian industrial facilities, 27 January 2016

focused on cybersecurity challenges faced by organisations in the energy sector found that 77% of the respondents noted that their organisation had experienced a rise in successful cyber-attacks in the last 12 months, and 68% said the rate of successful cyber-attacks had increased by over 20% in the last month.[20] Thus, there are growing concerns about the possibility of a cyber-attack causing physical damage, for example, an attack on the operating system could cause a malfunction resulting in loss of life, massive environmental damage, or shut-down or loss of assets, which would result in economic and financial disruptions.

### BOX 3: CYBER CROSSING OVER TO PHYSICAL

By exploiting industrial control systems and critical infrastructure, cyber-attacks now pose a threat to public safety and economic security. Within the energy sector, potential targets include offshore drilling rigs, power generation plants, and pipelines exposed by direct connectivity to the internet and enterprise IT networks.

Once inside the system, an infiltrator could, in theory, open an emergency shut-down valve, or adjust alarm system settings at a gas or petrochemical plant. The impacts of these acts could be significant, leading to fire or explosion and, consequently, damage to property, environmental harm, and/or loss of life. A cyber-attack on computer control or emergency shutdown systems, even at a small refinery, or petrochemicals or gas plant, could lead to fire or explosion worth hundreds of millions of dollars.[21] High accumulation losses can be triggered by a power failure because of possible widespread chain reactions. Targeted cyber-attacks on elements of the power grid could cause a power interruption. For example, a cyber-attack on the Distributed Energy Resource Management System could result in damage to transformers, which are expensive and often difficult to replace.[22]

Even if the damage resulting from an attack was localised, the business interruption exposure and values for an energy company could potentially run into billions of dollars as the wait for long lead-time components stretches into years as opposed to months. The variance in loss estimates differs much more greatly between offshore assets. For example, the complete loss of a platform could be anything from tens of millions of dollars to more than one billion, with business interruption at the top end running into several billions of dollars for every 12 months of lost production.[23]

To date, there has been limited large financial damage, physical damage or data theft across the energy industry and the sector has yet to experience catastrophic physical damage or a business interruption loss as a result of a cyber-attack. One survey suggests that critical infrastructure executives are possibly overconfident in their organisation's ability

[20] Tripwire Study, 2016: Energy Sector Sees Dramatic Rise in Successful Cyber Attacks, 7 April 2016
[21] Marsh, 2014: Advanced cyber-attacks on global energy facilities
[22] CRO Forum, 2014: Cyber resilience – The cyber risk challenge and the role of insurance
[23] Marsh, 2014: Advanced cyber-attacks on global energy facilities

to effectively respond to a cyber-attack; in a survey comparing perceived vulnerability to cyber risk between 2012 and 2015, energy executives revealed the greatest decrease in perceived vulnerability, from 53% to 24%.[24]

However, in the face of a dynamic threat, the energy sector will need to build and continually adapt its cyber resilience in order to ensure effective risk management in future energy infrastructure. This is particularly true for power utilities given the widespread reliance by all other sectors on a steady supply of power to maintain operations. This vital role in the supply chain makes power utilities a prime target for the most malicious of threats, including terrorists and adverse state actors.

## BOX 4: THE POTENTIAL COST OF MASSIVE CYBER-ATTACKS

A malfunction or an operational failure of energy infrastructure would have a cascading impact on other critical infrastructure (transportation, water supply) and across the economy (factories may have shut down to conserve energy). [25] For example, one study estimating that simultaneous malware attacks on 50 generators in the Northeast of the United States suggests this could cut power to as many as 93 million people, resulting in at least US$243bn – US$1trn in economic damage and US$21bn to US$71bn in insurance claims.[26] As a measure of comparison, the 2011 earthquake and tsunami in Japan caused US$300bn in economic damage, while the price tag for damages from Hurricane Sandy that hit the Northeast coast of the US in 2012 was almost US$100bn.

However, limited historical data and the constantly evolving threat make it a challenging peril to model. Models need to include a comprehensive catalogue of cyber scenarios from which insurers can derive frequency and severity distributions to measure the potential financial impact of loss from both affirmative cyber coverages and 'silent' all-risk policies where cyber is the peril, but no cyber exclusions exist. The systemic nature of the risk means that (re)insurers can suffer losses from multiple insureds across vast geographies from a single event, exposing infrastructure, supply chain, and other interconnected risks. A better understanding of the cyber aggregation potential can allow the further development of the cyber insurance market and uptake of cyber (re)insurance by the private sector.

[24] The Aspen Institute and Intel Security, 2015: Critical Infrastructure Readiness Report: Holding the Line Against Cyber threats
[25] Perez T, Segalis B and Navetta D, 2015; Energy cybersecurity – a critical concern for the nation, Data protection report (9 April 2015)
[26] Lloyds, 2015: Business Blackout: The insurance implications of a cyber attack on the US power grid

# TO BUILD CYBER RESILIENCE, EACH ORGANISATION MUST ANSWER A SIMPLE QUESTION: WHAT DO YOU HAVE TO LOSE?

# BUILDING RESILIENCE TO CYBER RISKS

Cyber risks are here to stay and attacks will continue to grow in frequency, sophistication and damage. Energy companies need to adopt a continuous pro-active approach to cyber resilience that goes beyond simply avoiding or responding to breaches in security and builds an organisation-wide resilience to cyber threats.

Traditionally cyber resilience focused on hardening the perimeter to protect against threats. Measures in cyber rely on technology to build protection. These measures include technology controls, attack surface minimisation, intrusion detection and prevention, malware detection and eradication, and encryption. Companies have also leveraged Big Data analytics to increase awareness of internal and external threats, as well as to enhance the understanding of anomalous network activity. However, it is not enough for companies to combat cyber threats within the confines of their organisational boundaries. In an age of online communication and transacting, building a ’hard shell‘ around the enterprise could cost more in lost business or inflated transaction costs than savings in reduced losses from cyber-attacks.

Traditional resilience must also be accompanied by a focus to mitigate the growing sophistication of modern cyber-attacks. Companies must develop an organisational response to resilience, one that uses both technology and human intuition to recognise and respond to cyber-attacks. This includes developing robust cyber governance, cyber-awareness culture and cyber-awareness behaviours within and between organisations. Human resilience is best increased by collaboration among multiple stakeholders to increase knowledge of cyber risks, and to raise the energy sector’s capabilities to prevent, detect and respond to cyber risks.

Building resilience to cyber threats requires organisations to first recognise cyber as a core risk to business continuity. Mitigating cyber risks completely will always be challenging, and it is not possible to build perfect cybersecurity; yet moving from a ’technology-only approach’ to resilience towards an ’organisation-wide approach’ will better protect energy systems from cyber risks. This will also help to better protect the communities in which energy infrastructures are located from accidental environmental, social, and financial damages.

# CALLS TO ACTION FOR STAKEHOLDERS

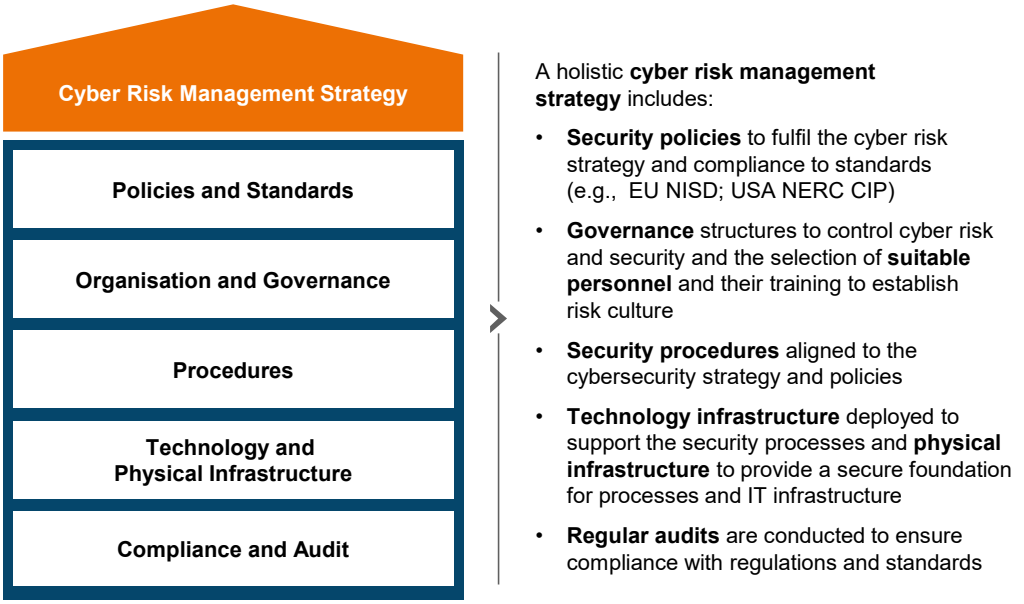
Multiple stakeholders have a role in helping the energy sector increase its resilience to cyber risks. The nature and changing risk profile of cyber threats demands a cross-industry, risk-based approach from businesses and governments around the world.[27]

Past cyber-attacks have shown that companies cannot face cybercrime alone. Instead, they must collaborate across the sector and across the public and private actors to be effective. Cyber risks should be faced at the industry level, as part of critical infrastructure protection programmes, with different companies developing and participating in cyber threat intelligence platforms together.

## Energy infrastructure operators

Companies must view the management of cyber risks in the same way as any other business risk, factoring in the necessary governance as well as scoping and quantifying the risk and the appropriate prioritisation of risk management resources. Increasing resilience to cyber risks requires the application of both traditional technology solutions and human controls and must be guided by a cyber risk management strategy (see Figure 2: A framework for a cyber risk management strategy).

### FIGURE 2: A FRAMEWORK FOR A CYBER RISK MANAGEMENT STRATEGY




Source: Oliver Wyman, 2014: A new approach to cybersecurity leveraging traditional risk management methods

[27] Marsh, 2014: Advanced cyber-attacks on global energy facilities

The adoption of a common cross-sector cybersecurity framework, such as the US's National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity can support the development of a comprehensive cybersecurity framework and create efficiencies, facilitate communication across energy supply chains and stakeholders, and locate key areas of cyber risk management.

### BOX 5: THE BATTLE FOR CYBERSECURITY TALENT

Cyber risk involves a level of complexity and a pace of change that exceed most other operational risks. Moreover, combatting cyber risks requires new skills and dedicated staff, and many energy companies are struggling to capture the right level of talent and integrate the talent across the organisation.

Maintaining cybersecurity, or information security, has become a top-tier issue for organisations in all sectors, and the team of employees, contractors, and/or external security service providers hired to keep company data secure has become a critical component of those organisations. The competition for talent in this field can be a decisive factor for organisational resiliency; as one energy executive acknowledged: "There is a deficit of cyber specialists in the energy industry to help companies prepare for cyber threats." The cybersecurity field is growing exponentially, and the demand for skilled workers exceeds the supply with a growth rate that is more than two times faster than all other IT jobs. Research has linked recent high-profile security breaches to the shortage of nearly one million skilled cybersecurity professionals. As a result, building a cybersecurity talent pool takes longer than other IT positions, and cybersecurity talent costs more than other IT positions.[28]

Companies should take an advanced approach to cyber risk management and priorities. Organisations must optimise investments in security technologies to balance risk and expense and ensure the most effective controls are protecting the most valuable corporate assets. It is essential that organisations clearly identify the business's most important information assets and data, namely information, products, areas, processes, or systems that are strategically relevant to the company and need to be protected at all costs.[29] Improving the understanding of how risks will impact business assets can help identify where companies need the best cyber protection. However, many organisations have challenges in determining their cyber weaknesses; few can provide a complete and up to date inventory of all asset equipment or have properly documented their core information technology assets – which include, for example, their databases, intellectual property, or computing resources. Many struggle to determine a complete list of all third party connections into their systems. As one energy executive interviewed noted: "To achieve cyber resilience, each organisation must answer a simple question: What do you have to lose? That is, what are the specific data, applications, or systems that are essential to conducting operations?"

[28] Mercer, 2015: Human Capital Challenges in a High Risk Environment: 2015 Cyber Security Talent Spot Poll
[29] Oliver Wyman, 2015: Closing The Door To Cyber Attacks: How Enterprises Can Implement Comprehensive Information Security

Answering that question with precision will enable businesses to begin developing a cybersecurity posture that is able to protect core functions while under duress.

Once they have identified key assets and data, management should clearly define their cyber risk appetite and quantify what value is at risk by identifying a range of likely outcomes on critical company assets, by quantifying the cost of cyber risk, and by taking a cost-benefit approach to risk mitigation. As with other operational risks, companies should set a target level of cybersecurity for all of their software, hardware, and employees based on their importance to the firm's overall appetite for risk. The companies should then ensure that controls and processes address gaps that are accordingly prioritised, starting with those that are mission critical.[30]

## BOX 6: CYBER RISK QUANTIFICATION

Robust risk quantification is essential for communicating risk, prioritising security safeguards, and allocating resources. For many companies, this currently means little more than a heat map representation of potential damage, which is often misleading, as it combines frequent small losses with rare large losses for each type of incident in the form of a single expectation of likelihood and impact.

A more reliable and functional approach is to build distributions, or risk curves, from whatever company-specific and industry-wide incident data is available by means of a Monte Carlo simulation. This approach has a number of benefits. It helps companies understand the range of outcomes and associated costs for each attack vector on a probabilistic basis. Application across attack vectors makes it possible to compare the different cost profiles and to determine which ones are causing the most losses overall. Monte Carlo simulations can reveal, for instance, that attack vectors that are low on the senior-level radar are in fact more troublesome than those of high concern.[31]

A definition of root causes that answer why a cyber incident happened supports the quantification and helps to better understand the vulnerability of any company.[32] Many organisations are also adopting another approach to quantifying cyber threats: cyber value-at-risk. This approach can enable organisations to make decisions regarding the appropriate amounts of investments in security systems by leveraging the complete cyber value-at-risk model and having a comprehensive outlook on the organisation's assets under threat.

The ability to adjust cost and incidence assumptions transparently enables risk managers to future-proof analyses based on current known trends. Not only can this type of modelling properly compare attack vectors on a like-for-like basis, but it can also support the aggregation of all cyber risks to quantify impact at an identified level of confidence. In turn, this aggregation can provide an analytical foundation for considering the acceptability of cyber risk levels for the organisation and discussing the value of risk transfer and

[30] Oliver Wyman, 2015: Will Hackers Cause The Next Energy Crisis?
[31] Marsh & McLennan Companies, 2016: Evolving Challenges In Cyber Risk Management Protecting Assets And Optimizing Expenditures
[32] For an example provided by the insurance industry, see CRO Forum, 2016: Concept paper on a proposed categorisation methodology for cyber risk, 14-16

mitigation investments.

Scenario analyses can be deployed using the same modelling technique to examine extreme events and emerging threats for which little data is available. 'What if'-type thinking is required to explore second- and third-order consequences, such as reputational impacts. In the section 'calls to action for stakeholders: insurance', two scenarios for the energy industry are presented.

Robust situational awareness and cyber risk analytics are vital in helping organisations identify vulnerabilities, rank threat scenarios, identify countermeasures, and set priorities for intelligence gathering. It is increasingly important to assess cyber risks across the entire energy value chain. 'Outside-in' risk assessments use scanning tools to examine how easy it is to penetrate a company system – through its web presence, stolen mobile devices and emails via firewall breaches, encryption failures, the exploitation of privileged accounts and general network porosity – and provide insight into how the system might be compromised.

Organisations must also consider how technological or software components built directly into control systems affect the operation of energy assets. As some energy executives observed, many companies must also address the issue that older IT systems may not have the necessary security and design standards for cyber resilience and may need to be improved. There may also be a need to diversify software product offerings within infrastructure designs in order to avoid 'monoculture risk'. This refers to the reliance on the use of single software across multiple infrastructures. Relying on one type of software increases the entry point for infiltration and also increases the likelihood that hackers could gain control of multiple system components.

Technology alone will not eliminate all cyber risks and companies must increase the focus on the human aspects of cybersecurity. Organisational culture, behaviour and processes play a critical role in reducing and managing cyber risks. Human or soft resilience measures begin with an effective governance structure and risk management framework, which includes integrating cybersecurity as a key issue in the governance process and a strategic issue at the top management level.

Cyber risks should be viewed as a core business risk across the entire enterprise, with risk management roles assigned to all departments, including the heads of IT, risk management, operations, finance, business and the CEO and the Board.[33] Cybersecurity must be embedded in business plans and operational activities from the outset rather than as an afterthought.

In particular, it is essential that cyber risk management and oversight is effectively allocated with consideration of roles and responsibilities between the IT departments, operations management, the Chief Information Security Officer, and other functions. For example, in many energy and power companies, ICS systems and other operational technologies may

[33] The IIA Research Foundation, 2014: Cybersecurity: What the board of directors needs to ask

be managed by the plants and operating companies whereas corporate applications and infrastructure will be managed by the IT department. In this scenario, it is critical that organisations have a clear cyber security governance model to drive cybersecurity updates across all areas of the organisation, and ensure that the cyber security measures are at the necessary and common level of maturity across the organisation.

Top managers in the energy industry need to develop a cyber risk management culture that becomes second nature to all employees from boards of directors to the frontline. One recent cross-industry survey of 1,530 non-executive directors, senior executives and others in the US, the UK, Germany, Japan, Denmark, Norway, Sweden and Finland reinforced this finding. The level of cyber awareness was low across the director and C-suite, with the lowest level of awareness in Japan, Nordic countries and Germany compared to the UK and the US.[34] Strong cultural awareness can be supported by embedding cyber risk management goals into performance targets, incentives, regular reporting, and key executive discussions.[35]

Companies must focus on education, training and regular corporate communications to ensure all employees have high cyber risk awareness. Cybersecurity must become everyone's responsibility − not just the IT department − but everyone from the board-level to general administrators. Many, if not most, cyber breaches can be traced back to human error.

End users are vulnerable to a variety of scams; for instance, 35% of employees across numerous sectors, including energy, chemical, and distribution, have been vulnerable to USB initiated attacks.[36] These small (conscious or not) human errors can have severe consequences. For example, it is estimated that more than 90% of successful cyber-attacks are launched via spear phishing campaigns, as one Chief Risk Officer noted in an interview.[37] It was a phishing scam sent to an employee that served as the entry point for the Ukraine power grid attacker. Employees must be trained in maintaining proper cyber risk management practices and in being vigilant and wary of potential breaches. Employees are often the best positioned to identify potential cyber-attacks as they are able to identify malfunctioning IT systems or processes.

Regularly testing cyber event response plans is also a way of ensuring high executive awareness of the severity and changing risk profile of cyber threats. Cyber event simulations are critical processes to test and improve an organisation's response capabilities, and many energy companies run annual events (see Box 7: Cyber event simulation).

[34] Tanium and NASDAQ, 2016: The Accountability Gap: Cybersecurity & Building a Culture of Responsibility
[35] Oliver Wyman, 2015: Will Hackers Cause The Next Energy Crisis?
[36] Verizon, 2015: Data Breach Investigations Report
[37] Hewlett Packard Enterprise, FireEye, and Marsh & McLennan Companies, 2016: Cyber resiliency in the Fourth Industrial Revolution: A roadmap for global leaders facing emerging cyber threats

## BOX 7: CYBER EVENT SIMULATION

In response to increased cyber threats, a US utility launched annual cyber event simulations in addition to drills required by federal regulations, to proactively prepare for and test their capacity to respond.

The company has conducted unique drills to stimulate cyber events which would have substantial ramifications for customers and business operations alike. Some examples of the drills include 'man in the middle', an insider data breach and theft of customer files.

These experiences in conducting the drills provide important lessons for other organisations conducting or planning to conduct such simulations.

**Simulations are an opportunity to increase cyber awareness across the organisation:** They provide an opportunity to educate employees to better understand cyber risks and consider the potential impacts on the company, its customers and the supply chain. The company has used internal and external experts, including law enforcement representatives, to provide employee learning sessions in preparation for the simulations.

**The process is designed to identify areas for improvement in cyber risk management:** Although focused on response actions, the simulations and preparations for the exercises have enabled the company to bolster its cyber defence mechanisms by exposing gaps in its ongoing cyber risk management practices.

**Involve a wide array of departments:** Cyber-attacks have a much wider business impact than other threats that the company simulates regularly, such as storm drills. For example, departments that would not normally be incorporated in storm drills, such as Investor Relations, must be included in cyber drills due to the widespread potential impacts of a cyber-attack. A range of business leads and functional leaders, including operations, investor relations, legal, and customer service in addition to information technology should be involved in the simulations.

**Involve key outside stakeholders:** The company invites several law enforcement agencies that would be likely to be involved in the response to any actual events, including the Federal Bureau of Investigation, the Department of Homeland Security, and local police departments, to participate alongside employees in the drills. The involvement of external participants enables employees to better understand the various roles and important hand-offs between law enforcement and company responsibilities in the event of a cyber-attack.

In terms of structuring and conducting cyber event simulations, the company's experiences reveal several important tips for effective drills:

- Provide clear structure: Simulations should be well-structured with clearly outlined roles.
- Enable adaptability and personalisation: Simulations cannot be scripted. Natural responses allow simulations to be in real-time and dynamic, thereby maximising business preparedness.
- Start small: Because smaller-scale events are easier to fully flesh out than bigger

ones, they are more useful for fully ascertaining the impacts of and business responses to cyber threats.

- Stay realistic: Participants will not be as engaged in a situation that they cannot imagine actually happening or cannot take seriously.

## Governments

Governments have recognised the economic threat presented by cyber risk and are taking a number of measures to build technological and human resilience across the economy and the energy sector. More than 30 countries – including Germany, Italy, France, the UK, the US, Japan, and Canada – have unveiled cybersecurity strategies. In February 2014, Chinese President Xi Jinping announced a new national cybersecurity body to coordinate security efforts, and in April 2015, Singapore launched a Cybersecurity Agency to oversee policies and conduct cybersecurity outreach. With these strategies, governments are supporting the development of cyber defences through support of research and innovation, knowledge and skill building, and by developing awareness of cyber risks. For example, the UK Government's Centre for the Protection of National Infrastructure provides good practice, technical guidance, and facilitates information exchange between sectors, including the energy sector and manufacturers of security equipment for national infrastructure.[38] France's cybersecurity strategies, coordinated by the National Agency for the Security of Information Systems, are similarly based on promoting cooperation between the public and the private sector.

Governments are also fostering collaborative sharing of information between the public and the private sector on cyber threats and vulnerabilities. Understanding the full cyber risk landscape is difficult for many firms and government-stimulated efforts (or industry association stimulated as discussed later) to support threat and response information can be very important. For example, the UK's Cyber Security Information Sharing Partnership was launched to support the wider objectives of the UK National Cyber Security Strategy. Such mechanisms enable companies to confidently and safely share information on cyber threats without revealing corporate vulnerabilities, corporate secrets, customers' personally identifiable information (PII), or leaving a company exposed to lawsuits, but also governmental or regulatory investigations. They also allow companies within the same industry to share information without concerns of apparent collusion. The benefits of cyber threat information sharing are well understood by the industry. As one energy executive interviewed for this report noted: "Companies need to cooperate better with each other and with governments to share experiences and best practices."

[38] National Technical Authority for Information Assurance, 2015: ICT Service Management: Security Considerations

Another important issue to consider is how to effectively share information on threats between the government and the security structure that helps protect countries and the private sector. Private sector actors may be reluctant to provide information if it is going to be shared with the security apparatus.

### BOX 8: EUROPE'S RESPONSE TO CYBERSECURITY

Europe's response to the issue of cybersecurity, the Network and Information Security Directive (NISD), becomes effective in 2018. NISD is an initiative and the first attempt to legislate in the cybersecurity arena, contrasting with the approach of other countries (for example, the US) which have opted for an industry-led/voluntary approach. In short, the NISD adopts a multi-layered approach by placing obligations on all stakeholders across the industry. It requires Member States to:

- Establish a national Network Information Security strategy and establish regulatory measures to achieve network security
- Establish a competent authority to monitor the application of NISD in their territory and across Member States
- Establish a Computer Emergency Response Team that handles incidents and risks

The European Commission and its member states must form a cooperation network which coordinates against the risks and incidents affecting network and information systems and circulates and exchanges information among members. The NISD requires "market operators" that provide "critical infrastructure", the "disruption or destruction of which would have a significant impact on a Member State", to comply with a mandatory security breach and incident notification requirement. "Market operators" are targeted cross-industry and include operators in the energy sector.

In many countries or regions existing approaches to cybersecurity compliance involve both mandatory and voluntary measures, depending on the sector. However, governments should be aware of the proliferation of overlapping regulations. For example, in the US, energy organisations often need to navigate a complex statutory and administrative landscape involving regulations, policy, and industry best practices. Some private grid operators with both electric and gas assets are required to comply with three different approaches to cybersecurity, with little congruency to each other. Electric utilities must abide by the mandatory North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, gas utilities have voluntary Pipeline Security Guidelines developed by the Transportation Security Administration, and facilities rated as being high risk by the Department of Homeland Security are regulated by the Chemical Facility Anti-Terrorism Standards.[39] In addition to critical infrastructure-specific standards, there is also a proliferation of standards and normative documents for the risk management

[39] National Grid, 2013: Digital Risk and Security Governance

of IT systems. For example, ISO/IEC 27032 is a generic, non-industry specific framework for information security that is accepted globally as a de facto standard.[40]

### BOX 9: THE HIGH COST TO MEET RISING CYBERSECURITY REQUIREMENTS

The US Federal Energy Regulatory Commission is taking steps to increase and enforce stringent cyber and physical security standards at utility companies that own and/or operate critical generation and transmission assets that power the nation. The CIP standards issued by the Federal regulator predominantly have widened in scope to include operational devices in generating plants and substations. For some large utilities, this can lead to a ten-fold increase in the number of devices that need to be protected. For example, one large utility developed a US$90m programme to update their cybersecurity measures to meet the CIP standards, another spent US$500m over five years to harden critical substations, and a third has asked regulators to grant the right to levy a special charge for cybersecurity.[41] Integrating cybersecurity updates into ongoing operations and maintenance is one mechanism companies are using to reduce the costs of implementing cybersecurity updates.

Cyber is a dynamic threat and organisations must be able to adopt security measures and approaches in response. Overlapping and competing regulations can result in an undue focus on meeting the minimum requirements and insufficient focus on responding to the threat.

Governments can also drive the establishment of cybersecurity standards. For example, the US NIST Cybersecurity Framework (see Box 10: Frameworks for improving critical information security) was developed with a view to international adoption; there is value for companies to have a globally consistent framework and standard to avoid confusion, duplication of effort, and/or conflicting expectations.[42] Italy, for example, has launched its own National Framework for Cybersecurity, borrowing heavily from the US Framework for Improving Critical Infrastructure Cybersecurity to ensure international harmonisation, and the EU Network and Information Security Directive has also adopted elements of the US NIST.[43] Australia is expected to leverage the NIST in developing a national policy. In the spring of 2016, Australia announced voluntary cybersecurity health checks at Australia's biggest companies as part of the government's overall cybersecurity strategy.

[40] Secuilibrium, 2014: Comparing NIST's Cybersecurity Framework with ISO/IEC 27001
[41] Bloomberg Technology, 2014: Hackers Find Open Back Door to Power Grid with Renewables
[42] Cyber Security Law & Practice, 2016: The global uptake of the NIST Cybersecurity Framework
[43] Cyber Intelligence and Information Security Center with Sapienza Universita di Roma, 2015: 2015 Italian Cyber Security Report

### BOX 10: FRAMEWORKS FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

In the US, the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity provides a common language with which the energy sector (and other sectors) can assess its cybersecurity readiness. Once the recommendations are implemented, organisations must continually review and update their policies. To help implement utilities the NIST framework, the US Department of Energy's Office of Electricity Delivery and Energy Reliability issued the Energy Sector Cybersecurity Framework Implementation Guidance in January 2015.[44]

It is important to note that the NIST Cybersecurity Framework is one of many emerging cybersecurity benchmarks in the US. For example, various existing NERC CIP standards are mandatory, which subjects the relevant regulated entities to potential enforcement action and penalty assessment. The North American Energy Standards Board (NAESB) has developed cybersecurity standards that are mandatory for various segments of the energy industry. In the case of natural gas companies, for example, NAESB's cybersecurity standards mandate the use of digital signatures and self-certification to support mutual entity authentication.[45]

Overall, governments have common goals in promoting cross-industry or industry-focused cyber security: to encourage businesses to adopt rigorous risk management practices commensurate to the threat, and to share information on the changing risk profile, thereby increasing awareness.[46]

Increasing international governmental cooperation in industrial cybersecurity issues will also help increase cross-sectorial and cross-border collaboration on cyberattacks. Considering common goals, it is essential to encourage the development of common frameworks also in inter-governmental organisations to introduce international standards for protection of energy systems against cyber-attacks.

## Industry associations

Around the world, energy companies, collaborating through industry associations, can work within the sector and with governments to define minimum technical rules and appropriate standards and measures required. Industry associations can serve as platforms for energy organisations to share information on vulnerabilities, and collaborate to continually strengthen cybersecurity practices by enabling benchmarking and best practices sharing within a given sector. A number of these already exist, for example in North America, the Electricity Information Sharing and Analysis Center (E-ISAC) provides pivotal services for early identification and detection owner and operator organisations of the Bulk Power System across North America. The value of better information shared was echoed by

[44] US Department of Energy, 2015: The Energy Sector Cybersecurity Framework Implementation Guidance
[45] Perez T, Segalis B and Navetta D, 2015; Energy cybersecurity – a critical concern for the nation, Data protection report (9 April 2015)
[46] Marsh, 2014: Advanced cyber-attacks on global energy facilities

energy executives interviewed for this report, who stressed: “Energy companies need to better communicate among themselves - we need to understand what other companies do with respect to cyber risks.”

The nuclear industry’s focus on continuously improving nuclear security practices, in part via peer reviews and training programmes conducted by the International Atomic Energy Agency (IAEA), the World Nuclear Association (WNA) and the World Institute for Nuclear Security, is one example that could be adopted by other energy sectors.

The nuclear sector’s strong focus on security has extended into cybersecurity. At the 2016 Nuclear Industry Summit, a working group of civilian nuclear energy companies released recommendations that associations such as the World Association of Nuclear Operators (WANO) and/or WNA establish regular discussions on cybersecurity issues, share good practices and cyber risk reduction strategies, while also taking into account national requirements for protecting sensitive information. The working group also recommended that the nuclear industry collaborate further with the IAEA to develop more cyber-focused guidelines and training for the nuclear industry.[47] Reaching a consensus on baseline good practices can help the nuclear industry, particularly in countries with fewer resources, to invest in cybersecurity and reduce the uncertainties associated with the rise of cybercrime and nuclear power.[48]

## Technology sector serving the energy sector

Technology vendors can play a critical role in furthering, or hindering, the resilience of energy infrastructures. These firms must ensure they deliver technologies that have security standards built into the products they are delivering. Security and innovation need to be developed hand-in-hand and planned for from idea inception to product rollout and beyond. Without doing so, ICS and SCADA controls can compound cyber risks, and increase the vulnerability of attack within energy operations (see Box 11: Bowman dam intrusion). In addition, employees awareness of cyber vulnerabilities within technologies that are used for day-to-day business operations must be included as part of an effective cybersecurity strategy.

### BOX 11: BOWMAN DAM INTRUSION

In 2013, a hacker breached the network of Bowman Avenue dam in Rye, New York by ’google dorking‘ a cellular modem, a method used widely by security experts and hackers alike to locate vulnerable hardware.[49] The breach was relatively minor: the attacker probed the back-office systems of the dam, which was a small structure used for flood control. The hacker was not able to control water functions as the dam’s sluice gates were not connected to the network at the time. Had the connection been operational, the attacker

[47] Nuclear Industry Summit, 2016: WG1 Report – Managing Cyber Threat
[48] Stimson Center, 2016: Nuclear Energy: Securing the Future
[49] CFO 2016: Iranian Hacker Used Google to Hack NY Dam Computer

could have remotely controlled water levels and flow rates, presenting a potential threat to the community's water security.[50]

The ease with which the hacker accessed back office systems of the dam raises concerns around the security of internet-connected control devices. It is argued that having devices linked through business networks rather than directly to the internet imposes additional time and effort on the hacker, affording the defender time to identify and address the intrusion.[51] Such minor breaches may be warning signs that hackers are conducting reconnaissance missions for larger projects, or establishing entry points into networks that can eventually facilitate the exploitation of more critical networks and systems.[52] Observers have also suggested that the target of the attack was intended to be the Bowman dam in Oregon, which serves as a key structure to agricultural irrigation.[53]

## BOX 12: SMART GRIDS AND CYBER RISKS

The proliferation of smart grid devices increases the potential for cyber exposures. It does not matter if those are small home devices − for example, wind and solar collectors − the risk of potential attack surface grows with every device connected to the grid. A particular vulnerability within smart grid architecture is concentrated on advanced metering infrastructure (AMI). AMIs, or devices like smart meters, are typically used to create an automated, two-way communication between consumers and utility providers. Smart grids and smart systems provide utility companies with real-time data about power consumption, and allow customers to make informed choices about their energy usage, based on the price of the time of use. Such systems are increasingly being rolled out as one mechanism to reduce greenhouse gas emissions through more efficient operation of the grid and enable optimal integration of distributed energy resource. For example, the UK is about to start a roll-out of 53 million smart meters into residences and small businesses by the end of 2020, Italy has rolled out 32 million smart meters and utilities in Romania, Russia, the Philippines, Hong Kong and China are also examining the technology.

Despite the operational benefits, the amount of information that companies hold in relation to their customers means that security breaches to these infrastructures now increase the cyber risks for the utility industry.

Furthermore, the security standards governing the AMI are in their infancy, primarily due to how electrical grids originated from de-centralised networks owned by local operators. In essence, security standards vary from utility to utility, as awareness of cyber threats varies among industry regulators. When merging smart grid technologies with more traditional grids, companies should focus on achieving synergy in security policies to ensure that the large amount of data that come from smart devices is secured and controlled. This would

[50] Perez E, Prokupecz S, 2016: US plans to publicly blame Iran for cyber breach, CNN (10 March 2016)
[51] Lee R, Assante M, Conway T, 2016: ICS 2016 Defense Use Case 4: Analysis of the recent reports of attacks on US infrastructure by Iranian actors
[52] Wylie D, 2016: Critical Infrastructure Takeaways from the Iranian Attack on NY Dam, Nexdefense (22 March 2016)
[53] Berger J, 2016: A dam, small and unsung, is caught up in an Iranian hacking case, The New York Times (25 March 2016)

include: protecting the advanced meters as end points; protecting the channels of communication; ensuring the identity of devices is managed; and monitoring and managing the users logging in.

## Insurance sector

Cyber insurance is one mechanism to help offset the potential financial impacts of a cyber-attack. Demand for this type of product in the energy sector, especially utilities has grown rapidly in the USA over the past three years, and is picking up throughout other regions, especially in Europe. Indeed, the UK and US governments among others are encouraging large and small companies alike to increase their cyber insurance coverage to effectively boost their overall resilience to cyber-attacks. Insurers should continue to develop appropriate cyber insurance products and learn how their existing portfolios are impacted by cyber incidents.[54]

### BOX 13: INSURANCE PROVIDERS FOCUS ON FIVE KEY QUESTIONS WHEN ASSESSING CYBER RISKS

1. Is an independent party reviewing, at a minimum annually, the effectiveness of the technical and organisational security controls and related processes?
2. Does the company have an overview of the critical information? Is this information adequately protected from end to end?
3. Does the company have organisational and technical controls in place to detect, respond, and react to a cyber-attack in good time, including cross-functional incident response structures and processes?
4. Does the company have regular security awareness activities and training to make employees aware of cyber risks and how to protect critical information?
5. Does the company have a governance structure in place that ensures that security controls are regularly assessed against the rapidly changing threat environment, and that the controls are adapted accordingly?

The process of applying for cyber insurance contributes to cyber risk management as it requires companies to assess their own cyber practices. The underwriting process includes an analysis of a company's technical defences, incident response plan, procedures for patching software, policies for limiting access to data and systems, monitoring of the vendor network, reporting on cyber risks and training of internal staff. In addition, carriers assess

[54] CRO Forum, 2016: Concept paper on a proposed categorisation methodology for cyber risk

the applicant's security practices (see Box 13: Insurance providers focus on five key questions when assessing cyber risks). Taken overall, the growing adoption of cyber insurance and the efforts of the individual companies to reduce cyber risks indicate that awareness of cyber risks is indeed increasing and driving behavioural change in the marketplace.[55]

Cyber insurance is a product that deals with a complex and continuously evolving risk. Broadly stated, three core components of cyber insurance currently provide financial relief after an incident:

1. Reimbursement of the costs a company pays to respond to a cyber incident. These expenses may come in the form of measures to comply with requirements to notify and protect affected individuals in the wake of a data breach, paying the expense to recreate corrupted or destroyed data

2. Coverage of fees and damages a company may have to pay in response to litigation resulting from a cyber incident

3. Reimbursement of revenues lost or expenses incurred due to a business disruption related to a cyber incident

Table 2 presents two examples for cyber risk core scenarios potentially affecting specifically the energy industry and how insurance can help address the financial impacts.[56] Appendix 2 lists all cyber incidents that could happen to any industry and potential insurance claims that could be made.

[55] HM Government and Marsh, 2015: UK Cyber Security: The Role of Insurance In Managing and Mitigating the Risk; and Testimony of Matthew P. McCabe, Senior Vice President, Marsh, LLC to the Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies (22 March 2016)
[56] Swiss Re, 2014: Gearing up for Cyber Risk

## TABLE 2: CYBER RISK CORE SCENARIOS

| Risk scenario | Blackout of energy supply following property damage | Fire/explosion |
|---|---|---|
| Scenario description | The infiltration of malware into an industrial control system via USB stick /internet provides the attackers with the ability to remotely control the infected processes.<br><br>A breakdown in a power plant (or power grid) due to malicious remote controlling by hackers leads to a large scale, long-lasting power outage, severe equipment damage, and affects infrastructure and services. | The infiltration of malware into an industrial control system via USB stick /internet provides the attackers with the ability to remotely control the infected processes.<br><br>A pressure increase due to malicious remote controlling by the hackers leads to an explosion/fire and destroys part of or the whole plant. |
| Industries affected | Electrical grid/power generation companies and all dependent systems<br><br>All industries dependent on energy supply | All industries, in particular critical infrastructures such as oil / gas, chemical / pharmaceutical, power generation, pipelines, storage |
| Consequences | Fire/explosion, machinery breakdown, business interruption, contingent business interruption, bodily injury, third party property damage, environmental damage, loss of profits/bankruptcy leading to shareholder claims | Destruction of plant, business interruption following fire/explosion, contingent business interruption, bodily injury, third party property damage, environmental damage, loss of profits/bankruptcy leading to shareholder claims |
| Potential contingent business interruption (CBI) claims | Outage of several power plants can be compensated (low CBI)<br><br>Outage of a large number of plants may result in large CBI, e.g., supply bottleneck to repair power plants, partial shortage of electrical power over certain period | Outage of several refineries /plants can be compensated (no/low CBI)<br><br>Outage of large number of plants may result in large CBI e.g., interruption of plastic production |
| Potential insurance claims | Property/engineering, workers' compensation and employers' liability, general/product liability (incl. pollution liability), directors and officers | Property/engineering, workers' compensation and employers' liability, general/product liability (incl. pollution liability), directors and officers |

Source: Swiss Re, 2016

However one should note that cyber events in utilities or oil and gas companies can be difficult to assess, as they may have complex origins and a wide range of potential impacts. For example:

- a malfunction and physical damage in a pipeline could cross multiple national boundaries,
- it may be difficult to prove that a given physical breakdown was caused by a cyber-attack,
- malicious viruses can lie dormant in operating systems for a number of years, leading to questions of whether the cyber-attack should be considered to have occurred on the date of infection or the date the damage was observed.

Traditional insurance policies in the energy sector broadly exclude damage and consequential loss from cyber-attack and even where some form of cover is provided other policy exclusions may apply in the event of a cyber-attack. The exclusions effectively rule out financial means for recovery of damages or liability expenses following a cyber event. This creates a large uninsured risk for the energy industry, especially considering that the loss of operating control of key equipment could have catastrophic effects, such as fire, explosion or machinery breakdown that can lead to loss of machinery, human injury and other critical impacts.

Cyber events can also create significant interruption to business. In the energy industry, business interruption exposures are a vital threat as replacing damaged infrastructure can take two years or longer. This stands in contrast to other industries, such as internet sales businesses, which are more concerned about being offline for a few hours or days. The significance of potential business interruptions in the energy industry suggests that cyber insurance is essential for energy companies when exposures run into billions of dollars and the available limits are much lower.

Because cyber is still an emerging risk, there is limited history insurers can draw upon to calculate the premium. Insurers will therefore continue to maintain a conservative approach to underwriting cyber risks until the confidence level is higher and cyber insurability has increased. In general, this can be achieved through collaboration within the energy industry and its subsectors.

Cyber breaches are fuelling interest in and placement of some cyber-related risks in captive insurers and a recent study found that the use of captives for cyber risks grew 30% in 2015.[57] A captive is an insurance company owned by a non-insurance company and used to finance the parent company's retained risk.

[57] Among Marsh-managed captives, cyber liability is the third fastest growing non-traditional risk in captive utilisation, growing 30% 2014-2015. Over the past four years, cyber liability programs in Marsh captives, both new and existing, have grown by 160%. See Marsh 2016: Captive Solutions: Creating Security in an Uncertain World

Although there is limited use of captives for cyber risks in the energy sector, there has been increasing interest from the industry. As companies are forced to retain more cyber risk, a captive serves as an attractive tool that can quickly respond in the event of a catastrophic loss, helping to lower cash flow volatility and provide budget stability.

For extreme scenarios like a complete breakdown of infrastructure, such as an entire power grid, grid operators must be integrated into a protection strategy to also enhance insurability across borders.[58]

### BOX 14: CYBER TERRORISM INSURANCE

Terrorism remains an excluded peril in almost all property policies and is typically defined as “an act, including the use of force or violence, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organisation(s), committed for political, religious or ideological purposes”. It is clear that many cyber-attacks could well fall within this definition and be considered acts of terrorism. Accordingly, no matter how broad the cyber coverage is under the insured’s property policy, no indemnity will be provided if a given cyber-attack is ruled to be terrorism. As a result demand for standalone cyber terrorism insurance is on the rise. Current insurance plans that address this need include limits of up to US$400m and subscribe to the same definition of terrorism in order to provide dovetailed coverage for both property damage and business interruption.

The insurance market for cyber energy risks is growing, but the energy industry has still to improve its understanding of the risk and of the insurance options available. Energy companies have, so far, exhibited a varied level of response to the cyber threat and available insurance options. It is expected that as the sector becomes subject to more risk management scrutiny, risk transfers will increasingly be seen as a necessity − especially as more cyber insurance products become available and the risk continues to grow.

[58] ibid

**CYBER RISKS ARE GROWING IN TERMS OF BOTH THEIR SOPHISTICATION AND THE FREQUENCY OF ATTACKS.**

# CONCLUSION

Cyber risks are growing in terms of both their sophistication and the frequency of attacks. Today's cyber risk landscape shows that the aggressive nature of this risk requires energy firms to reconsider how they view and address cyber risks within their organisations.

In order to effectively mitigate cyber risks, companies should take a cross-sectorial, risk-based approach to evolve their focus from prevention of cyber risks to developing a comprehensive operational strategy. This requires recognising that cyber risk is not limited to an IT problem, but that this risk must be approached as an enterprise-wide concern to ensure effective risk management. Energy companies should also ensure that the technology providers they are working with embed security features directly into their products from the outset.

Energy assets do not operate in isolation, but instead, act as a critical component to the core functioning of economies and societies. By broadening the understanding of which assets may be affected and better estimating how much business continuity may be disrupted, energy firms can gain a better quantified understanding of their cyber risks. The energy sector can work together by supporting industry associations and collaborating with governments to ensure that these critical infrastructures are protected to a safe standard.

Understanding the nature of impacts can help companies gain a better quantified understanding of how and where cyber-attacks are likely to disrupt their business. Insurance can then help to fill the protection gap. However, the lack of historical data related to cyber risks also makes it difficult for insurers to calculate their premiums. More detailed information from the energy sector will help the insurance industry to improve their coverage of energy assets, and the diversity of their product offerings.

# Appendices

# APPENDIX 1: CYBER RISK – A GLOSSARY OF SELECTED COMMON TERMS[59]

The following are some commonly used terms when discussing cyber risk and cyber risk management in the energy sector.

**Attack:** An attempt to gain unauthorised access to system services, resources, or information, or an attempt to compromise system integrity.

**Black hat:** A black hat is a computer hacker who works to harm others (e.g., steal identities, spread computer viruses, install bot software).

**Cyber extortion:** ransom or investigative expenses associated with a threat directed at the client to release, divulge, disseminate, destroy, steal, or use confidential information taken from the client, introduce malicious code into the company's computer system; corrupt, damage or destroy company's computer system, or restrict or hinder access to the company's computer system.

**Cyber terrorism:** A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

**Distributed denial of service (DDoS) attack:** A DDos attack is the disabling of a targeted website or Internet connection by flooding it with such high levels of Internet traffic that it can no longer respond to normal connection requests. Often mounted by directing an army of zombie computers to connect to the targeted site simultaneously, the targeted site may crash while trying to respond to an overwhelming number of connections requests or it may be disabled because all available bandwidth and/or computing resources are tied up responding to the attack requests

**Disruption:** An event which causes unplanned interruption in operations or functions for an unacceptable length of time.

**Endpoint protection:** In network security, endpoint security refers to a methodology of protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connecting to the network creates a potential entry point for security threats.

[59] National Initiative for Cybersecurity Careers and Studies within US Department of Homeland Security's Office of Cybersecurity and Communications, 2016: Glossary of common cybersecurity terminology; Harvard University, Berkman Center for Internet and Society, 2016: Cybersecurity glossary

**Hacker:** An unauthorised user who attempts to or gains access to an information system

**Hacktivism:** The nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development.

**Incident:** An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

**Industrial control system (ICS):** An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets.

**Malware:** A variety of computer software designed to infiltrate a user's computer specifically for malicious purposes. Includes, inter alia, computer virus software, botnet software, computer worms, spyware, Trojan horses, crimeware and rootkits.

**Phishing (spear):** The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entityor person in an electronic communication.

**Supervisory control and data acquisition (SCADA) Systems:** SCADA in the cybersecurity context usually refers to industrial control systems that control infrastructure such as electrical power transmission and distribution, water treatment and distribution, wastewater collection and treatment, oil and gas pipelines and large communication systems. The focus is on whether as these systems are connected to the public Internet they become vulnerable to a remote attack.

**Sponsored attacks:** Computer network attacks commissioned by, supported by or carried out by a state, government or governmental agency.

**System integrity:** The attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorised manipulation of the system.

**Trojan:** Malware that masquerades as some other type of program such as a link to a web site, a desirable image, etc. to trick a user into installing it.

**Two factor authentications:** Authentication using two factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

**Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**Worm:** A type of malware that replicates itself and spreads to other computers through network connections.

# APPENDIX 2: POTENTIAL CYBER INCIDENTS AND INSURANCE CLAIMS

## TABLE 3: POTENTIAL CYBER INCIDENTS AND INSURANCE CLAIMS

| Incident type group | | Insurance overage scope |
|---|---|---|
| 1 | Business interruption/ Interruption of operations | Reimbursement of lost profits caused by a production interruption not originating from physical damage |
| 2 | Contingent business interruption (CBI) for non-physical damage | Reimbursement of the lost profits for the observed company caused by related third parties (supplier, partner, provider, customer) production interruption not originating from physical damage |
| 3 | Data and software loss | Costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted or encrypted |
| 4 | Financial theft and/or fraud | Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets (e.g., shares). It covers both pure financial losses suffered by the observed company or by related third-parties as a result of proven wrong-doing by the observed company |
| 5 | Cyber ransom and extortion | Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment (e.g., access to data is locked until ransom is paid) |
| 6 | Intellectual property theft | Loss of value of an Intellectual Property asset, resulting in pure financial loss |
| 7 | Incident response costs | Compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defense costs.<br><br>Coverage includes: IT investigation and forensic analysis, excluding those directly related to regulatory and legal defences costs, public relations, communication costs, remediation costs (e.g., costs to delete or cost to activate a 'flooding' of the harmful contents published against an insured), notification costs |

| Incident type group | | Coverage scope |
|---|---|---|
| 8 | Breach of privacy | Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incidents response costs |
| 9 | Network security/Security failure | Compensation costs for damages caused to third parties (supplier, partner, provider, and customer) through the policyholder/observed company's IT network, but excluding incidents response costs. The policyholder/observed company may not have any damage but has been used as a vector or channel to reach the third party |
| 10 | Reputational damage (excluding legal protection) | Compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company |
| 11 | Regulatory & legal defense costs (excluding fines and penalties) | A: Regulatory costs: compensation for costs incurred to the observed company or related third-parties when responding to governmental or regulatory inquiries relating to a cyberattack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes Fines and Penalties).<br>B: Legal Defense costs: coverage for own defense costs incurred to the observed company or related third-parties facing legal action in courts following a cyber-attack. |
| 12 | Fine and penalties | Compensations for fines and penalties imposed on the observed company. Insurance recoveries for these costs are provided only in jurisdictions where it is allowed |
| 13 | Communication and media | Compensation costs due to misuse of communication media at the observed company resulting in defamation, libel or slander of third parties including web-page defacement, as well as Patent/Copyright infringement and Trade Secret Misappropriation |
| 14 | Legal protection – lawyer fees | Costs of legal action brought by or against the policyholder, including lawyer fees costs in case of trial. Example: identity theft, lawyer costs to prove the misuse of victim's identity |

| | Incident type group | Coverage scope |
|---|---|---|
| 15 | Assistance coverage – psychological support | Assistance and psychological support to the victim after a cyber-event leading to the circulation of prejudicial information on the policyholder without his/her consent |
| 16 | Products | Compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber-event, excluding technical products or operations (Tech E&O) and excluding Professional Services E&O |
| 17 | D&O | Compensation costs in case of claims made by a third party against the observed company' directors and officers, including breach of trust or breach of duty resulting from cyber event |
| 18 | Tech E&O | Compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber-event |
| 19 | Professional services E&O, professional indemnity | Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber-event, excluding technical services and products (Tech E&O) |
| 20 | Environmental damage | Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber-event |
| 21 | Physical asset damage | Losses (including business interruption and contingent business interruption) related to the destruction of physical property of the observed company due to a cyber-event at this company |
| 22 | Bodily injury and death | Compensation costs for bodily injury or consecutive death through the wrong-doing or negligence of the observed company or related third parties (e.g. sensible data leakage leading to suicide) |

Source: CRO Forum, 2016: Concept paper on a proposed categorisation methodology for cyber risk

# ACKNOWLEDGEMENTS

The project team would like to thank the individuals who informed the project's approach, supplied information, provided ideas, and reviewed drafts. Their support and insights have made a major contribution to the development of the report.

## PRINCIPAL CONTRIBUTORS AND INTERVIEWEE'S

Jeoren van der Veer (Executive Chair)

*(Note: organised by countries' alphabetical order)*

Raimo Peterson, Estonia; Victoria Hennequart, France; Jacque Sibue, France; Carlo Bozzoli, Italy; Stefano Buschi, Italy; Paolo D'Ermo, Italy; Laura Pilla, Italy; Ferruccio Bellelli, Italy; Roberto Simeone, Italy; Simonetta Sabatino, Italy; Alessandro Cleirici, Italy; Dudley Baylis, South Africa; Dave Collins, South Africa; Barry McColl, South Africa; Alejandro Villar, Spain; Matthew Holt, United Kingdom; Filipe de Mota da Silva, United Kingdom; Barbara Tyran, United States

## WORLD ENERGY COUNCIL STUDIES COMMITTEE

Brian Statham, South Africa (Chair)

*(Note: organised by countries' alphabetical order)*

William D'haeseleer, Belgium; Claudia Cronenbold, Bolivia; Eduardo Correia, Brazil; Jing Ding, China; Bin Wei, China; Qinhua Xu, China; Yaxiong Zhang, China; Li Zhu, China; Jean-Paul Bouttes, France; Rauno Rintamaa, Finland; Jeanne Ng, Hong Kong; B P Rao, India; Atsushi Noda, Japan; Nastaran Rahimi, Iran; Alessandro Costa, Italy; Carlo Papa, Italy; Hardiv Situmeang, Indonesia; Arturo Vaca, Mexico; Jan Antonczyk, Poland; Ioan Dan Gheorghiu, Romania; Ayed Qahtani, Saudi Arabia; Maria Sunér Fleming, Sweden

## MARSH &MCLENNAN COMPANIES CONTRIBUTORS

Francois Austin (Partner, Oliver Wyman); Amy Barnes (Managing Director, Marsh); Raj Bector (Partner, Oliver Wyman); Leslie Chacko (Principal, Oliver Wyman); David Christensen (Senior Sales Leader, Marsh); Alan Feibelman (Partner, Oliver Wyman); Tom Fuhrman ( Managing Director, Marsh Risk Consulting); Michael Gaudet (Managing Director, Marsh USA, Inc.); Andrew George (Energy and Power Chairman, Marsh); Bernhard Hartmann (Partner, Oliver Wyman); Claus Herbolzheimer (Partner, Oliver Wyman); Andrew Herring, (Managing Director, Marsh); Anneloes Hesen (Senior Project Manager, Marsh); Tom Jacob (Product Development Leader, Mercer); Jose Maldonado (Business Analyst, Marsh); Matthew McCabe (Senior Vice President, Marsh); Robert Parisi (Senior Advisory Specialist, Cyber, Marsh); Jeremy S Platt (Senior Vice President, Guy Carpenter); Thomas Reagan (Practice Leader, Cyber, Marsh); Angelo Rosiello (Principal, Oliver Wyman); Karen Shellenback (Senior Network Consultant, Mercer); Stella Tse (Senior Client Advisor , Marsh); Luc Vignancour (Senior Client Advisor, Marsh)

## SWISS RE ADVISORS AND PRINCIPAL CONTRIBUTORS

Philippe Aerni (Head Fin Pro P&C and Special Lines, Swiss Re Corporate Solutions), Guido Benz (Director, Swiss Re Corporate Solutions), François Brisson (Head Cyber Technology, Swiss Re Corporate Solutions), Markus Buergi (Vice President Swiss Re Communications), Maya Bundt (Head Cyber & Digital Strategy, Swiss Re), Eric Durand (Director, Swiss Re Group Underwriting), Martin Hegelbach (Director, Swiss Re Corporate Solutions), Urs Leimbacher (Director, Swiss Re), Stephan Schreckenberg (Director, Swiss Re), Willy Stoessel (Head Cyber, Technology & Construction, Swiss Re Corporate Solutions), Rey Leclerc Sveinsson (Vice President, Cyber Strategy & Risk Services, Swiss Re)

## PROJECT TEAM

Jereon van der Veer, (Chair, Resilience, World Energy Council); Christoph Frei (Secretary General, World Energy Council); Juerg Trueb (Managing Director, Head of Environmental Commodities and Markets, Swiss Re Corporate Solutions); Alex Wittenberg (Executive Director, Global Risk Center, Marsh & McLennan Companies); Didier Sire (Senior Advisor to the Secretary General, Head of Sectoral Programmes, World Energy Council)

## AUTHORS/PROJECT MANAGEMENT

Lucy Nottingham (Director, Global Risk Center, Marsh & McLennan Companies), Oliver Schelske (Senior Risk Research Manager, Swiss Re Centre for Global Dialogue, Group Strategy), Bernd Wilke (Vice President, Swiss Re Communications), Aida Boll (Vice President, Swiss Re Communications), Sandra Winkler (Director Policies, World Energy Council), Einari Kisel (Senior Project Manager, World Energy Council), Katrina Kelly (Project Manager, Financing Resilient Energy Infrastructure)

# OFFICERS OF THE WORLD ENERGY COUNCIL

**MARIE - JOSÉ NADEAU**
Chair

**YOUNGHOON DAVID KIM**
Co-chair

**MATAR AL NEYADI**
Vice Chair – Special Responsibility
Gulf States/Middle East

**NUER BAIKELI**
Vice Chair – Asia

**KLAUS-DIETER BARBKNECHT**
Vice Chair – Finance

**LEONHARD BIRNBAUM**
Vice Chair – Europe

**OLEG BUDARGIN**
Vice Chair – Responsibility for
Regional Development

**JOSÉ DA COSTA CARVALHO NETO**
Chair – Programme Committee

**JEAN-MARIE DAUGER**
Chair – Communications & Strategy Committee

**HASAN MURAT MERCAN**
Vice Chair – 2016 Congress, Istanbul

**BONANG MOHALE**
Vice Chair – Africa

**SHIGERU MURAKI**
Vice Chair – Asia Pacific/South Asia

**O.H. (DEAN) OSKVIG**
Vice Chair – North America

**BRIAN A. STATHAM**
Chair – Studies Committee

**JOSÉ ANTONIO VARGAS LLERAS**
Vice Chair – Latin America/Caribbean

---

**CHRISTOPH FREI**
Secretary General

## PATRONS OF THE WORLD ENERGY COUNCIL

Accenture Strategy
Bloomberg New Energy Finance
Electricité de France
Emirates Nuclear Energy Corporation
ENGIE
GE Power
Hydro-Québec
Korea Electric Power Corp.
Marsh & McLennan Companies
Masdar
Oliver Wyman
PricewaterhouseCoopers
Siemens AG
Swiss Re Corporate Solutions
Tokyo Electric Power Co.
VNG – Verbundnetz Gas AG

**World Energy Perspective – The road to resilience: managing cyber risks**
Published by the World Energy Council (2016) in partnership with Marsh & McLennan Companies and Swiss Re Corporate Solutions.



World Energy Council, Company Limited by Guarantee
Registered in England and Wales No. 4184478, VAT Reg. No. GB 123 3802 48
Registered Office 62–64 Cornhill, London EC3V 3NH, United Kingdom

**ISBN: 978 0 946121 53 3**

## WORLD ENERGY COUNCIL

Algeria
Argentina
Armenia
Austria
Bahrain
Belgium
Bolivia
Botswana
Brazil
Bulgaria
Cameroon
Canada
Chad
Chile
China
Colombia
Congo (Dem. Rep.)
Côte d'Ivoire
Croatia
Cyprus
Czech Republic
Denmark
Ecuador
Egypt (Arab Rep.)
Estonia
Ethiopia
Finland
France
Germany
Ghana
Greece
Hong Kong, China
Iceland
India
Iran (Islamic Rep.)
Iraq
Ireland
Israel
Italy
Japan
Jordan
Kazakhstan
Kenya
Korea (Rep.)
Kuwait
Latvia
Lebanon
Libya
Lithuania
Luxembourg
Malaysia
Mexico
Monaco
Mongolia
Morocco
Namibia
Nepal
Netherlands
New Zealand
Niger
Nigeria
Pakistan
Paraguay
Peru
Philippines
Poland
Portugal
Qatar
Romania
Russian Federation
Saudi Arabia
Senegal
Serbia
Singapore
Slovakia
Slovenia
South Africa
Spain
Sri Lanka
Swaziland
Sweden
Switzerland
Syria (Arab Rep.)
Tanzania
Thailand
Trinidad & Tobago
Tunisia
Turkey
Ukraine
United Arab Emirates
United Kingdom
United States
Uruguay
Zimbabwe

62–64 Cornhill
London EC3V 3NH
United Kingdom
T (+44) 20 7734 5996
F (+44) 20 7734 5926
E info@worldenergy.org

**www.worldenergy.org | @WECouncil**