WORLD ENERGY COUNCIL

World Energy Perspectives | 2016

EXECUTIVE SUMMARY

IN PARTNERSHIP WITH MARSH & MCLENNAN COMPANIES AND SWISS RE CORPORATE SOLUTIONS

THE ROAD TO RESILIENCE – MANAGING CYBER RISKS

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 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 a highly attractive target for 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 cyber security 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.

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.

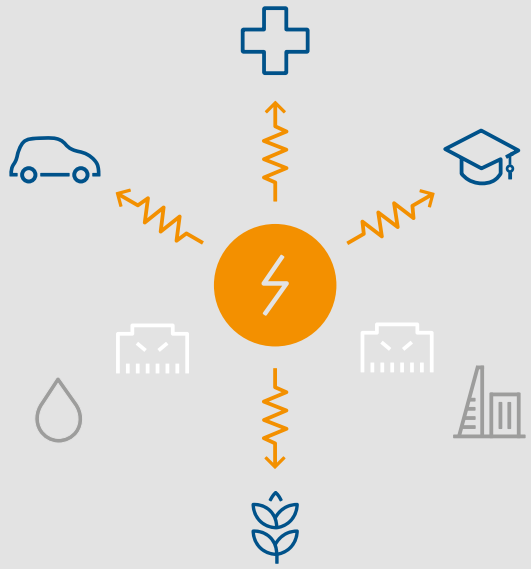
Companies should implement measures to prevent, detect and respond to cyber threats. This includes both technical measures of resilience (security measures for software and hardware, measures governing physical structures, such as limiting access to data centres, and clear instructions for using external 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.

THE ROAD TO RESILIENCE: MANAGING CYBER RISKS

ENERGY INFRASTRUCTURE: THE HEART OF ALL MODERN ECONOMIES

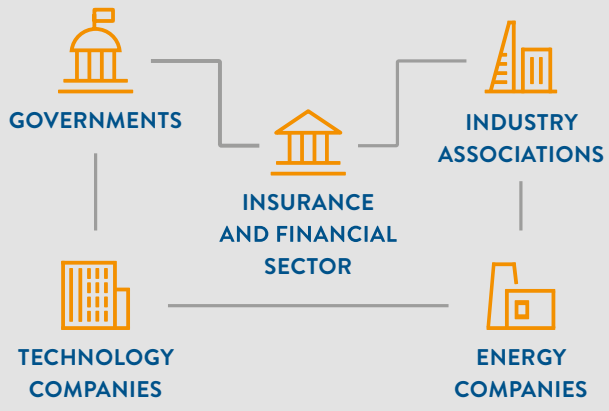


Cyber risks are growing in terms of both their sophistication and the frequency of attacks. The economic and physical consequences of cyber-attacks on energy infrastructure could be severe, making it an attractive target.

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

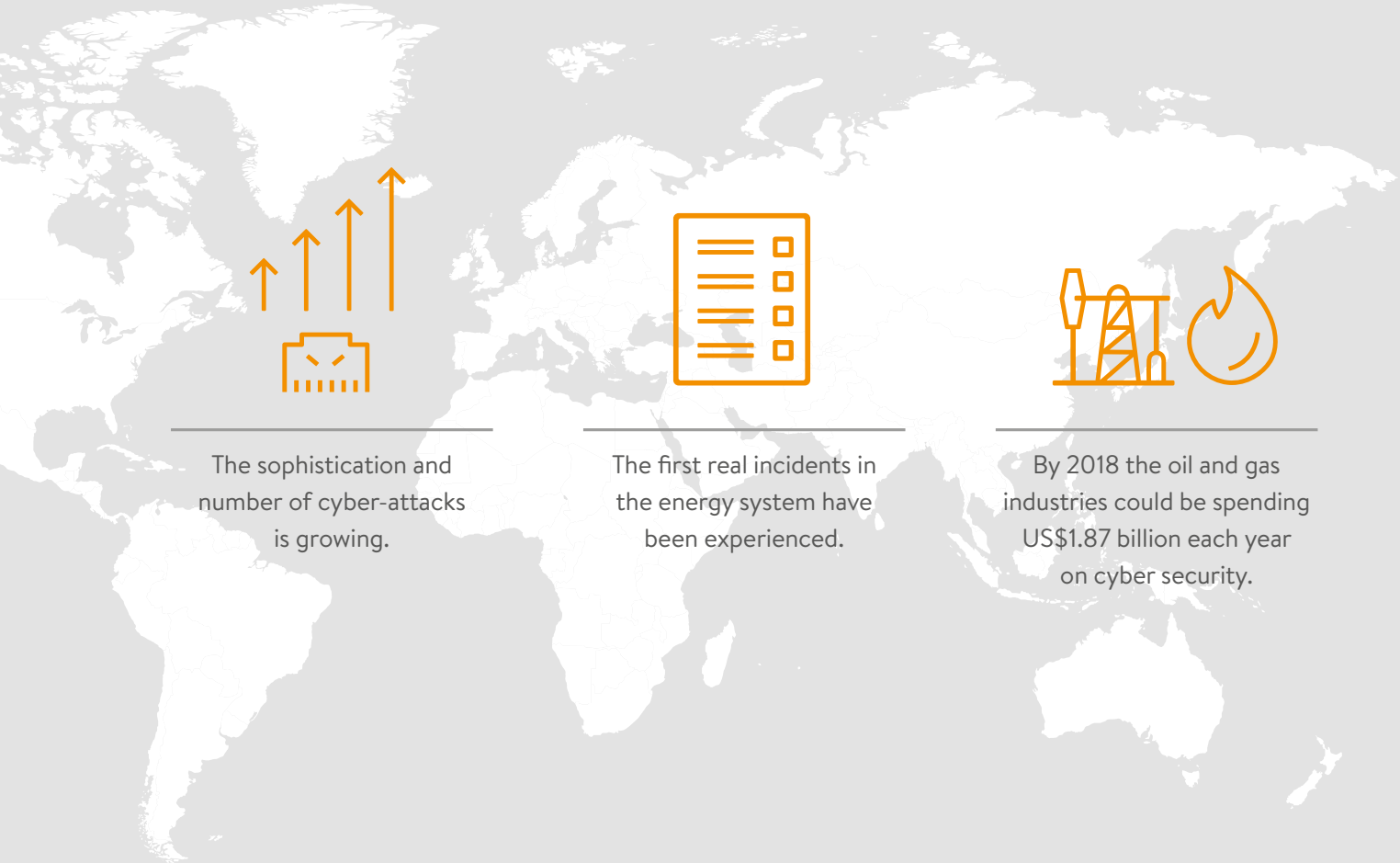
Korea Hydro and Nuclear Power Co. suffered a series of attacks aimed at causing nuclear reactors to malfunction. The attacks only succeeded in leaking non-classified documents.

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.

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 needs.

- **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 is 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.

ABOUT THIS REPORT

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.

DISCLAIMER

WORLD ENERGY COUNCIL

The World Energy Council is the principal impartial network of energy leaders and practitioners promoting an affordable, stable and environmentally sensitive energy system for the greatest benefit of all. We are the UN-accredited global energy body, representing the entire energy spectrum, with member organisations in over 90 countries.

Further details at **www.worldenergy.org** and **@WECouncil**

The full report can be found at **www.worldenergy.org/publications**

Published by the World Energy Council 2016

www.worldenergy.org

World Energy Council
Registered in England and Wales
No. 4184478

VAT Reg. No. GB 123 3802 48

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

ISBN: 978 0 946121 53 3