U.S. Resilience Project

**LITERATURE REVIEW**

A Scan of Reports Assessing Risks of Energy Disruptions for Businesses

Debbie van Opstal

# Key Risks to Business from Energy Disruptions

The literature on energy risks typically takes either a national perspective — disruptions to the energy system or specific infrastructure — or an infrastructure owner perspective. But, the literature on energy disruption largely lacks a framework for understanding risks to businesses from disruptions in the energy infrastructure, or how interdependencies between infrastructures could impact business continuity more broadly. Traditionally, energy risks to businesses have been profiled through a financial, rather than operational, lens — defined in terms of market price and volatility, procurement and purchasing practices, supply and demand forecasts, regulatory requirements and tax rates for alternative fuels. More recently, carbon footprint has been added as an energy risk.

The climate change discussion has opened a new conversation on the business continuity challenges of disruptions to energy infrastructure. But, the initial wave of reports appears aimed at building consensus that there is a problem rather than documenting and quantifying risks.

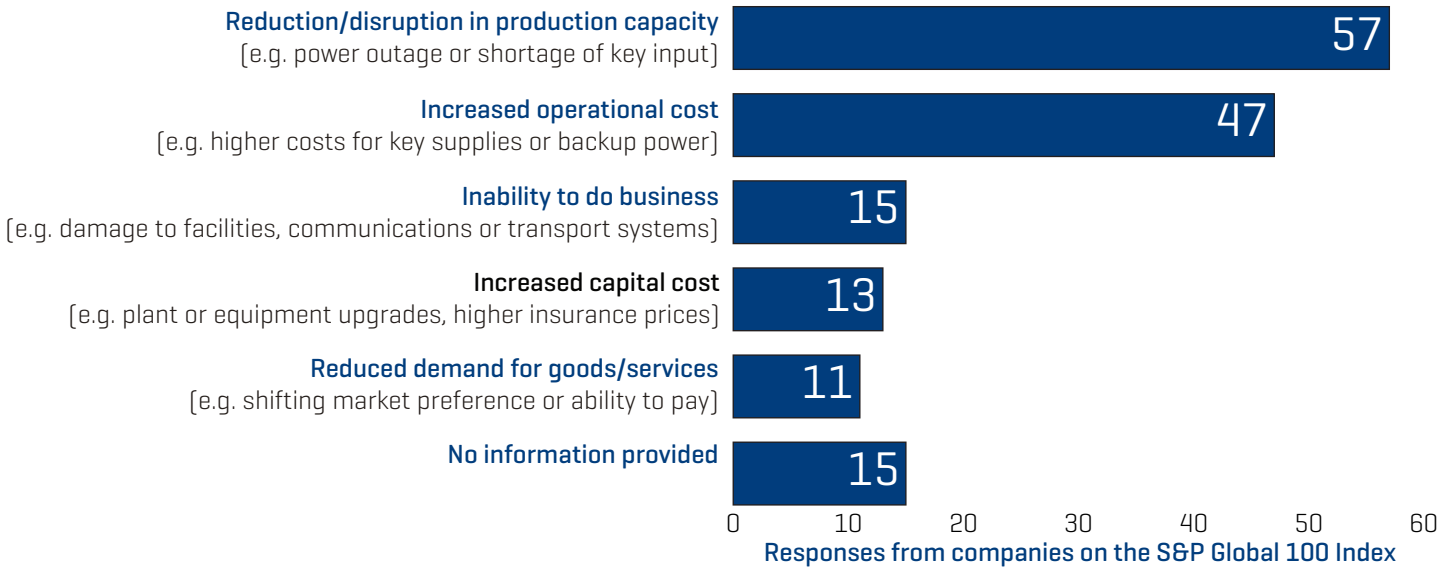
*The U.S. Resilience Project is grateful to the U.S. Department of Energy for sponsoring this analysis. In particular, the USRP would like to acknowledge Senior Technical Advisor Alice Lippert for her vision in seeking to understand energy risks from the business perspective.*

## Weathering the Storm: Building Business Resilience to Climate Change

*Center for Climate and Energy Solutions*[1]
*July 15, 2013*

Nearly all — 90 percent — of S&P Global 100 Index companies identify the impact of extreme weather on climate change as current or future business risk, across all industry sectors. A key risk is the disruption in production capacity caused by energy disruptions.

### Business Risks from Extreme Weather




### Recommendations for Business Resilience by Business

- Create a clearing house for reliable, up-to-date analytical tools. Companies need user-friendly localized projections of climate changes and models that link projections to impacts germane to company operations.
- Invest in public infrastructure resilience. Companies rely on public resources — including roads, bridges, and ports to get their goods and services to market — and need these resources to withstand extreme weather and climate impacts.
- Consider resilience needs in regulation. Companies in regulated sectors, such as water, electricity and insurance need regulators to be forward-looking and open to companies making the case for more spending on resilience.
- Set up voluntary, public-private partnerships bringing together government and business focusing on improving resilience planning.

## Sustainable Energy Security: Strategic risks and opportunities for business

*Lloyds of London and Chatham House*[2]
*2010*

### Summary Findings on Emerging Energy Risks to Business

- Businesses which prepare for and take advantage of the new energy reality will prosper. Failure to do so could be catastrophic. Energy security and climate change concerns are unleashing a wave of policy initiatives and investments around the world that will fundamentally alter the way that we manage and use energy. Companies which are able to plan for and take advantage of this new energy reality will increase both their resilience and competitiveness. Failure to do so could lead to expensive and potentially catastrophic consequences.

- Market dynamics and environmental factors mean business can no longer only rely on low cost traditional energy sources. Modern society has been built on the back of access to relatively cheap, combustible, carbon-based energy sources. Three factors render that model outdated: 1. surging energy consumption in emerging economies, 2. multiple constraints on conventional fuel production, and 3. international recognition that continuing to release carbon dioxide into the atmosphere will cause climate chaos.

- Energy infrastructure will become increasingly vulnerable as a result of climate change and operations in harsher environments. Much of the world's energy infrastructure lies in areas that will be increasingly subject to severe weather events caused by climate change. On top of this, extraction is increasingly taking place in more severe environments such as the Arctic and ultra-deep water. For energy investors, this means long-term planning based on a changing, rather than a stable climate. For energy users, it means greater likelihood of power and fuel supply disruptions.

- Businesses must address energy-related risks to the supply chain and the increasing vulnerability of "just-in-time" models. Businesses must address the impact of energy and carbon constraints holistically, and throughout their supply chains. Tight profit margins on food products, for example, will make some current sources unprofitable as the price of fuel rises and local suppliers become more competitive. Retail industries will need to either re-evaluate the "just-in-time" business model which assumes a ready supply of energy throughout the supply chain or increase the resilience of their logistics against supply disruptions and higher prices. Failure to do so will increase a business's vulnerability to reputational damage and potential losses resulting from the inability to deliver products and services in the event of an energy crisis.

## Forum on the Climate-Energy Security Nexus: Implications for Business

*IEA*[3]
*2012*

The Forum is a group of companies from the energy, manufacturing and financial sectors, along with government representatives brought together for an exploratory discussion on the impacts of a changing climate and how energy-related sectors could enhance their resilience to these impacts.

### Challenges

- Lack of a strong narrative to rationalize action on resilience in the short term
- Clear documentation of current climate impacts and resiliency solution options
- Definition of climate change resilience vis-à-vis adaptability
- Explanation of the trade-off between short-term spend and long-term risk hedging/ cost-effectiveness
- Lack of a strong economic argument for resilience, emphasizing collateral benefits of adaptation measures
- Need for "thought leadership" to develop a new resiliency paradigm for stakeholders.

### Needs

1. Better data is urgently needed
   - Is all the necessary information being gathered currently by research centers?
   - Meteorological projection data needs to be better circulated to interested parties; connect research centers and weather centers to governments and industry
2. Costs of inaction to a sector needs to be better characterized and modelled. Companies may be reluctant to share data on possible costs of inaction for fear of compromising competitiveness — this concern needs to be addressed

## Advanced Cyber Attacks on Global Energy Facilities

*Marsh Risk Management Research*[4]
*March 2014*

Although the article specifically addresses energy owners, the implications of the insurance policy exclusion for cyberattacks are that losses incurred from energy disruptions caused by cyberattacks will not be covered in business interruption insurance policies — not just for infrastructure owners, but for any company. The inability to insure against certain types of losses stemming from energy disruptions has not been widely discussed elsewhere in the literature.

In the two years from 2009-2011, General Keith Alexander noted that the United States had experienced a 17-fold increase in cyber attacks. In the first six months of 2013, there were more than 800 regulatory filings that mentioned cyber-related risks, representing a 106 percent increase over the same period in 2012. According to DHS, 53 percent of the 200 incidents responded to by ICS CERT between October 2012 and May 2013 were directed at energy facilities. To put that in perspective, the second highest target was manufacturing, which was the target for 17 percent of the attacks.

Cyberattacks against energy facilities could have profound repercussions economically. Since 2003, cyberattacks have been a standard insurance policy exclusion:

> "In no case shall this insurance cover loss damage, liability or expense, directly or indirectly caused by or contributed to, by or arising from the use or operation, as a means of inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system."

### Insurance Industry Assessments of Energy Risks

Insurance industry assessments of risk often point to gaps in business coverage as a result of emerging risks (power outages, cyber, climate change risks) or unanticipated risks to insurers. In the latter category, for example, the World Trade Center event gave rise to major losses in more than 20 different classes of insurance — not just the property damage or business interruption losses. The WTC was the world's first worker's compensation and life insurance catastrophe and the world's largest insured art loss.

## Power Trip, Emerging Risks

*Allianz Insurance*[5]
*No date provided*

Allianz Insurance did a special risk issue on the risks of power blackouts. Analyses from blackout events in the United States show that a 30-minute power cut results in an average loss of U.S.$15,709 for medium and large industrial clients, and nearly U.S.$94,000 for an 8-hour interruption. Even short blackouts — which occur several times a year in the United States — add up to an annual estimated economic loss of between U.S.$104–$164 billion.

The past decade has seen two of the costliest power blackouts and business interruption events. On August 14, 2003 large portions of the Midwest and northeast United States and Ontario, Canada, experienced an electric power blackout when a power line hit trees that lasted for up to four days in some areas. The U.S. Department of Energy put the cost at U.S.$6 billion — the majority of which were business losses. Canada is estimated to have seen its gross domestic product reduced by 0.7 percent for the month of August as a direct result of the blackout, with a net loss of 18.9 million working hours.

Manufacturing industries were particularly hard hit. Car manufacturer DaimlerChrysler lost production at 14 of its 31 plants and had to scrap 10,000 vehicles because there was no power to dry the cars going through the paint shops. At Ford Motor Company's casting plant in Brook Park, Ohio, the outage caused molten metal to cool and solidify inside one of the plant's furnaces, which delayed production by one week.

The earthquake and tsunami in Japan in March 2011 forced many companies to relocate operations and to source materials from other suppliers. Sony was forced to shut down five of its six laptop battery factories, while Hitachi closed its LCD Tokyo factory because of damage and power cuts.

Michael Bruch, Risk Consultant at Allianz Global Corporate & Specialty (AGCS), says that organizations need to check their vulnerability to power blackouts and what contingencies they have in place. He also believes that companies need to make sure that the various risk scenarios of power failures are clearly included in their business continuity management (BCM) strategies and those scenarios and mitigation solutions are regularly tested. "Controlling that risk should not just be limited to having emergency back-up generators or being able to relocate their operations and workforce — it also needs to take into account the effect that a power cut could have on their supply chains as well. Risk managers need to ensure that their suppliers have equally robust measures in place as well."

**Cost Analysis of Historic Blackout Scenarios — Industry typical financial loss per event**
Source: Copper Development Association

**Semiconductor Production**
3,800,000 Euros

**Financial Trading**
6,000,000 Euros
(per hour)

**Computer Center**
750,000 Euros

**Telecommunications**
30,000 Euros
(per minute)

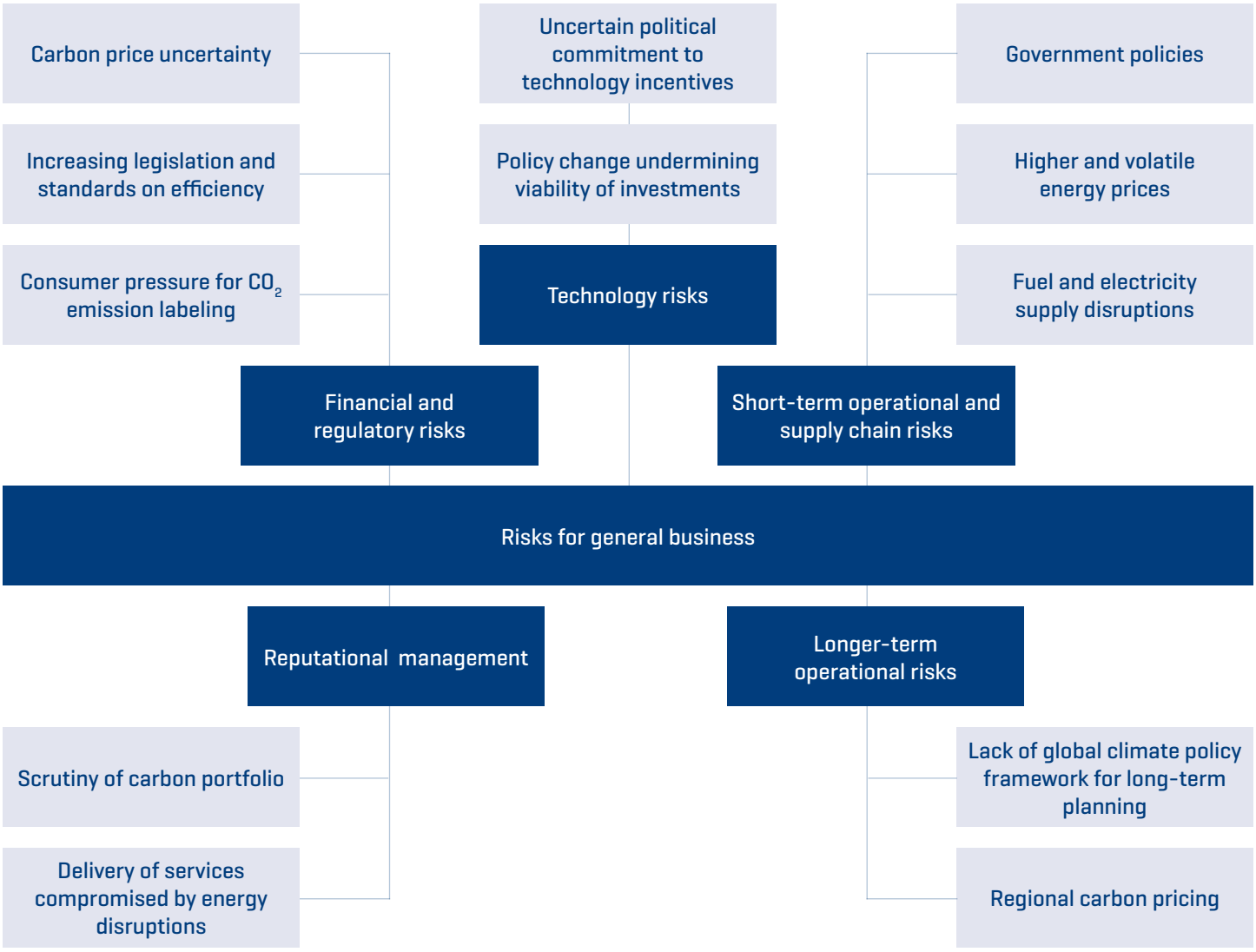
**Steel Works**
350,000 Euros

**Glass Industry**
250,000 Euros

## Insurance Framework for Business Risks from Energy Disruptions

*Lloyds of London*[6]

### Risks for the Wider Business Sector



## International Risk Assessment of Energy Security
## The IEA Model of Short Term Energy Security

*Jessica Jewell*[7]
*2011*

The framework developed by the IEA (MOSES) identified the four A's of energy risk: Availability (geological), Accessibility (geopolitical), Affordability (economic) and Acceptability (environmental and social). Its framework set up a four quadrant analysis between external and internal risks and resilience capability.

Dimensions of energy security addressed in the IEA MOSES Framework

| | Risks | Resilience |
|---|---|---|
| **External** | Risks associated with potential disruptions of energy imports. | Ability to respond to disruptions of energy imports by substituting with other suppliers and supply routes. |
| **Domestic** | Risks arising in connection with domestic production and transformation of energy. | Domestic ability to respond to disruptions in energy supply such as fuel stocks. |

Indicators for Risk and Resilience in the Moses Framework

| Energy Source | Dimension | | Indicator |
|---|---|---|---|
| **Crude oil** | External | Risk | Net import dependence |
| | | | Political stability of suppliers |
| | | Resilience | Entry points (ports and pipelines) |
| | | | Diversity of suppliers |
| | Domestic | Risk | Proportion of offshore production |
| | | | Volatility of domestic production |
| | | Resilience | Average storage level |
| **Oil products** | External | Risk | Oil product net import dependence |
| | | Resilience | Diversity of suppliers |
| | | | Entry points (ports, rivers and pipelines) |
| | Domestic | Risk | Number of refineries |
| | | Resilience | Flexibility of refining infrastructure |
| | | | Average stock levels |

| Energy Source | Dimension | | Indicator |
|---|---|---|---|
| **Natural gas** | External | Risk | Net import dependence |
| | | | Political stability of suppliers |
| | | Resilience | Entry points (LNG ports and pipelines) |
| | | | Diversity of suppliers |
| | Domestic | Risk | Proportion of offshore production |
| | | Resilience | Daily send-put capacity from underground and LNG storage |
| | | | Natural gas intensity |
| **Coal** | External | Risk | Net import dependence |
| | | | Political stability of suppliers |
| | | Resilience | Entry points (ports and railways) |
| | | | Diversity of suppliers |
| | Domestic | Risk | Proportion of mining that is underground |
| **Biomass and waste** | External | Risk | Net import dependence |
| | Domestic | Resilience | Diversity of sources |
| **Biofuels** | External | Risk | Net import dependence |
| | | Resilience | Entry points (ports) |
| | Domestic | Risk | Volatility of agricultural output |
| **Hydropower** | Domestic | Risk/ Resilience | Annual volatility of production |
| **Nuclear power** | Domestic | Risk | Unplanned outage rate |
| | | | Average age of nuclear power plants |
| | | Resilience | Diversity of reactor models |
| | | | Number of nuclear power plants |

## End Notes

1. http://www.c2es.org/publications/weathering-storm-building-business-resilience-climate-change
2. http://www.manicore.com/fichiers/LLoyds_Chatam_House_froggatt_lahn.pdf
3. http://www.iea.org/media/workshops/2013/nexus/nexus2_summary_report_june13.pdf
4. http://spain.marsh.com/Portals/52/Documents/Cyber%20Risk-%202014_Final.pdf
5. http://www.agcs.allianz.com/insights/expert-risk-articles/energy-risks/
6. http://www.manicore.com/fichiers/LLoyds_Chatam_House_froggatt_lahn.pdf
7. http://www.iea.org/publications/freepublications/publication/moses_paper.pdf