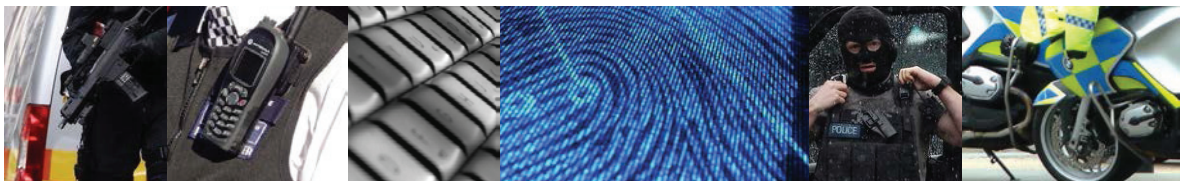
London First

‘Energy Security Keeping the lights on: A guide for security and resilience managers’

Roundtable – 20 March 2014

Sponsored and Hosted by Google



ENERGY SECURITY KEEPING THE LIGHTS ON: A GUIDE FOR SECURITY AND RESILIENCE MANAGERS

On 20 March 2014 a breakfast briefing was held by London First on the topic of 'Energy Security – Keeping the lights on: A guide for security and resilience managers'. The event was kindly hosted by Google.

The briefing was hosted by Richard Steel, Regional Data Centre Security Manager, European Operations, at Google, and chaired by Robert Hall, Director, Security and Resilience Network at London First. The event was programmed around a series of short presentations from:

- **Mark Pollard**, Managing Director, Europe Industry Practices, Marsh Inc.
- **Mark Prouse**, Energy Resilience, Department of Energy and Climate Change

KEEPING THE LIGHTS ON

As the country's electricity supply faces its biggest strain in years, emergency measures are being designed to prevent blackouts and brownouts (rostering) across Britain. The consequences of any cuts for industry in particular and businesses in general could be severe. This briefing outlined both the issues and possible responses, and looked at specific actions that risk, security and resilience managers could undertake in advance.

SYSTEMIC VULNERABILITIES AND MICRO RISKS

In an age where global resources are becoming increasingly scarce, where the effects of global climate change are becoming alarmingly self-evident, and where geopolitical relations grow fragile and exposed, concerns over ensuring the continuity of electrical power supplies are emerging as a salient security concern in the 21st Century. These security risks can be broadly categorised into three key areas of concern:

I. Evolution of the Power System: Regulatory and Operational Uncertainties

Coined as a 'Trilemma' by The World Energy Council, there are three factors which underpin energy sustainability:

- **Energy Security**. Can we rely on an uninterrupted energy supply? Power regulators all over the world remain fundamentally concerned with ensuring that electrical power is available on demand at the customer's convenience.

- **Energy Equity**. Can people and industry afford electricity? Power regulators need to ensure that electricity remains an affordable commodity and prevent it from becoming a luxury item.

- **Environmental Sustainability**. Can energy providers achieve demand-side efficiency and carbon dioxide reduction? While supply and affordability had been under control for decades, concerns over climate risk arose approximately 10 years ago as evidence from the global scientific community began to emerge.

Recognising the importance of environmental sustainability, energy security and energy equity became a secondary concern for power regulators. Concentrating on European countries, such as Germany and Spain, regulatory focus shifted to incentivising the energy industry to invest in nascent technologies and renewable energy.

While power regulators were largely successful in encouraging a dramatic increase in the use of renewable energy in countries such as Germany, other European countries have lagged behind the curve largely due to a number of problems that have developed in the wake of this shift.

- **The cost of renewable energy technology has fallen**. Today, solar panels cost a fraction of the price a decade ago, gear-box technology used for wind energy is considerably safer and the resolution of early technical faults throughout the industry means that the now reliable technology has reduced in cost. Industry subsidies, however, have remained broadly the same which attracts high margins in some parts of the world, and yet they are perceived to be at risk. Lack of investor confidence, therefore, is a big challenge to the development of security in the power industry.

- **The majority of sources for renewable energy are intermittent**. As such, conventional power stations need to remain operational in order to fill in the gaps in service provision and balance the networks. However, conventional power stations are designed to be base load plants which should be operational all the time in order to achieve maximum efficiency in terms of both function and cost. The problem, therefore, is that as renewable energy networks expand and grow the necessity for conventional power stations decreases. Operating below their full capacity conventional power stations become expensive and inefficient. Consequently, there needs to be investment which is channelled into developing a more efficient use of power both in terms of storage and distribution. At present, energy storage on an industrial scale doesn't exist and batteries only provide a short-term solution.

II. CYBER RISK: MALICIOUS OR ACCIDENTAL

As the power industry has evolved over the last decade a systemic issue has developed from the increasing software dependency of power generation and delivery across the industry. While countries such as Italy have experienced increased efficiency through their transition to smart metering – a system which remains controlled by a private network but which transmits meter readings via to the internet – the prospect of increasing online connectivity through smart grids has escalated concerns over network vulnerability.

Prior to their connection to the internet, the cyber-security risk to power generation, transmission and distribution networks remained relatively modest. However, since going online the opportunity for hacker s to gain access to power control systems via external doors has meant that security requirements have increased dramatically. As the intrinsic security of these networks was not designed to mitigate the cyber-threats of the modern age, power distribution businesses which are connected online are finding it increasingly difficult to obtain insurance due to their failure to comply with minimum security requirements.

As more appliances go online the security threats posed by distributed denial-of-service (DDoS) attacks holds the potential to place a crippling load on the power grid, seriously damaging the balance between supply and demand in a network.

III. CLIMATE RISK

In the last decade the issue of climate change and the importance of switching to renewable energy have been at the top of the agenda within the power industry. The meteorological events which have hit the UK in the last 12 months have served as a reminder that the global change in climate can have a detrimental effect on the UK's power supply and critical infrastructure. Storms which swept across the UK's western coastlines and river towns in October 2013 left 600,000 homes without power, highlighting the need for greater resilience within the energy industry.

In addition to changes in the global climate, the energy industry also faces threats from the outside of the Earth's atmosphere. 'Space weather', which was observed in 1859 during what is now commonly referred to as the Carrington Event, saw a solar flare hit the Earth's magnetosphere, inducing the largest known geomagnetic storm ever recorded. Estimated to occur within a returning period of 150 years, a report produced by Lloyd's of London ventured that a repeat of this solar activity within the Earth's atmosphere today could produce an estimated upper limit of $2.6 trillion in damage to power networks and infrastructure in the US alone.

GOVERNMENT POSITION AND BUSINESS RESPONSE

At present, the UK government considers pandemic influenza, coastal flooding, catastrophic terrorist attacks and volcanic eruptions to be amongst the highest priority risks that face national security. While all of these events have a potential effect on the energy sector, there are a number of specific and significant risks that have a direct impact on the industry, the largest being technical failure of the national grid, severe weather, space weather, cyber-attacks, and terrorist attacks on critical infrastructure. These risks have been determined through a collaborative effort between Government, the energy sector, as well as OFGEM - the industry regulators – to identify potential threats, to understand how they might manifest and how they can be proportionately mitigated.

While there are many possible levels of disruption that can result from any such threat, from a business perspective, even the smallest of risks can have a highly detrimental effect on their ability to operate normally. Government, however, will only involve itself directly in instances where it believes it can add value to response operations which is usually decided within COBR (Cabinet Office Briefing Room) meetings where emergencies are assessed, potential responses are explored, and where Government decides how and whether it can facilitate and improve emergency efforts. Ultimately, subsidiarity remains central the UK's strategy in handling such emergencies and any government decisions to intervene will be deferred to a specific Government department, for example DEFRA (Department for Environmental and Rural Affairs), which will co-ordinate response efforts down to the lowest local level of decision-making.

The possibility of there being a national loss of energy supply, however, is incredibly low with the National Grid having a certified 99.99998% reliability rate. If such an event were to occur, local businesses should expect to be without power from anywhere between 3 and 5 days, and possibly considerably longer depending on the cause of the disruption and the extent of the damage experienced during the event. Contingencies for regional and national power outages remain largely reliant on the 'Black Start' procedure - a National Grid process for recovery which initiates the creation of 'power islands' that allow power to regenerate and spread forming a skeletal transmission network.